Verifying Cellular Network Operations On Your Phones: From Simulation to Practice

Chunyi Peng

Purdue University

IEEE GLOBECOM 2017 Tutorial

December 2017

This Tutorial: Agenda

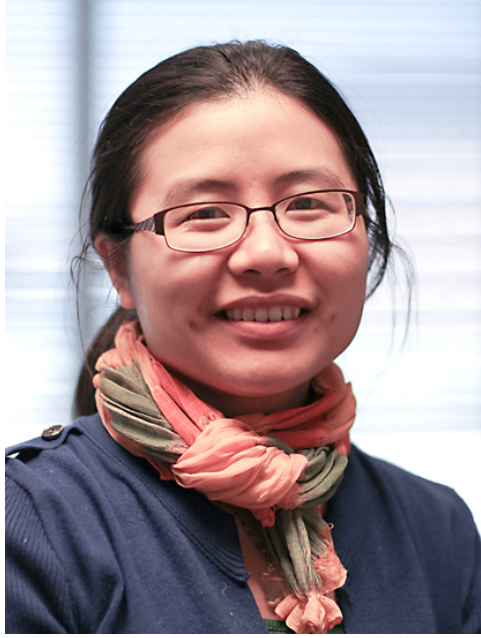
1. Introduction
2. Tutorial overview
3. MobileInsight: first look
4. Primer on cellular protocols
5. MobileInsight: second look
6. Research opportunities and examples
7. Advanced topics
8. Closing remarks

Introduction

Please introduce yourself

- ❑ Name
- ❑ Affiliation
- ❑ Research interests & projects
- ❑ Expectations
- ❑ One hobby or fun fact

Introduction



- Name: Chunyi Peng
- Affiliation: Purdue University
  - 2017/08~ , Assistant professor @Purdue
  - 2013/08~2017/08, Assistant professor @Ohio State
  - 2009/09~2013/06, PhD @ UCLA
- Research interests & projects
  - 5G/4G mobile networking: protocol, performance & reliability
  - Project: Mobile network intelligence (networking & AI)
- Expectations
  - Towards a community of practical mobile network research
- One hobby or fun fact

Introduction

Please introduce yourself

- ❑ Name
- ❑ Affiliation
- ❑ Research interests & projects
- ❑ Expectations
- ❑ One hobby or fun fact

Before We Start

- MobileInsight
  - http://www.mobileinsight.net
- Android app on rooted phones
  - Use phones in my lab
  - Or install it on your phones if rooted (V3.3)
  - http://www.mobileinsight.net/download.html
- Developers (next, if interested)
  - Setup (~ 30 minutes)

Install Development Environment

- http://mobileinsight.net/mi-dev-vm.html
- Install all-in-one VM package (for developers only)
  - Install Virtualbox and Vagrant;
  - Download the MobileInsight's vagrant script (https://github.com/mobile-insight/mobileinsight-dev)
  - Create a folder and install it (~ 30 minutes)
    - > cd MI_FOLDER
    - > vagrant destroy *# Run it only if you have installed VM before*
    - > vagrant up
    - > vagrant ssh

source codes in /home/vagrant/mi-dev

This Tutorial: Agenda

1. ✓ Introduction
2. ⬇ **Tutorial overview**
3. MobileInsight: first look
4. Primer on cellular protocols
5. MobileInsight: second look
6. Research opportunities and examples
7. Advanced topics
8. Closing remarks

What is No.1 Disruptive Technology in the Past 10 Years?

What is No.1 Disruptive Technology in the Past 10 Years?

9 January 2007

Picture: https://commons.wikimedia.org/wiki/File:Steve_Jobs_presents_iPhone.jpg

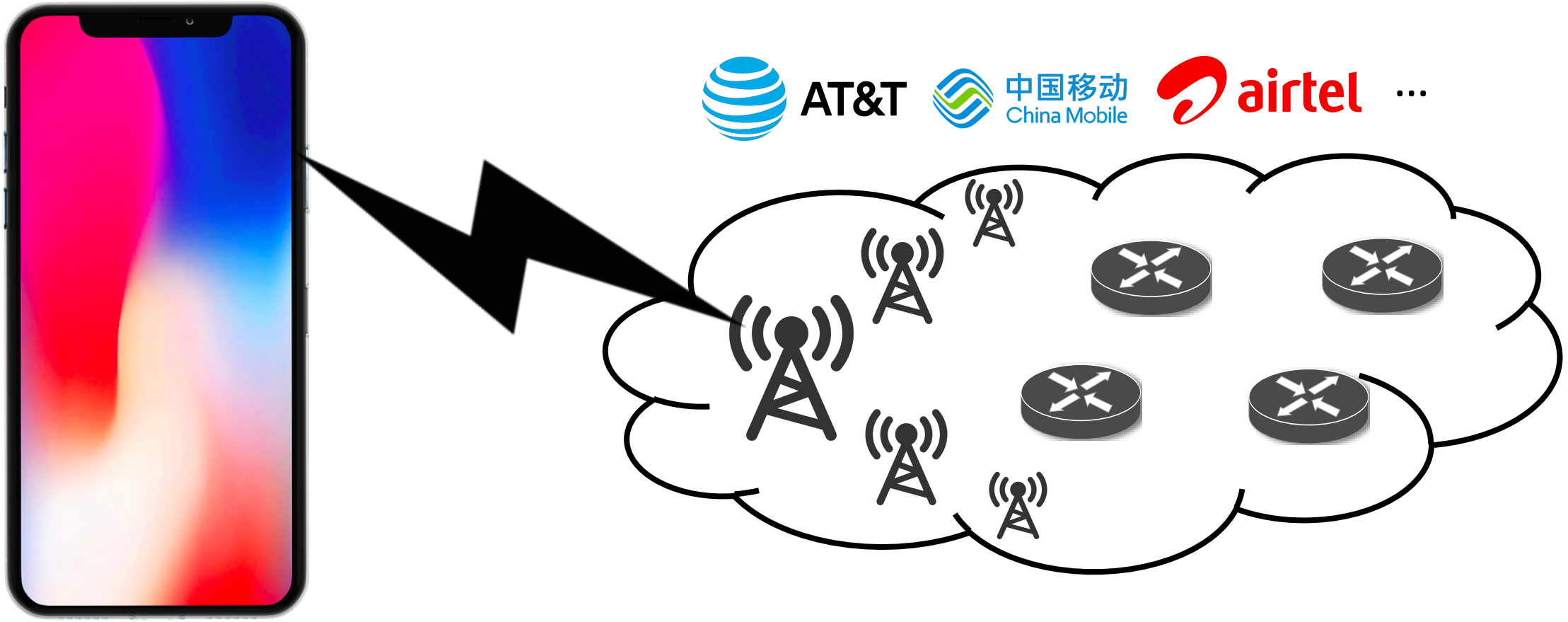
What is No.1 Disruptive Technology in the Past 10 Years?

9 January 2007

3 November 2017

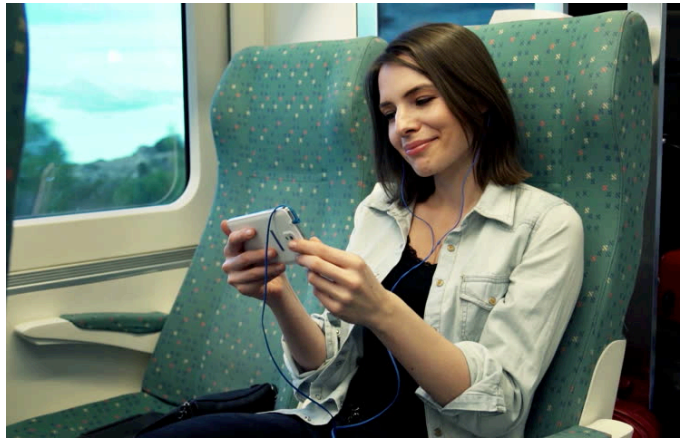
Picture: https://commons.wikimedia.org/wiki/File:Steve_Jobs_presents_iPhone.jpg

What is No.1 Disruptive Technology in the Past 10 Years?

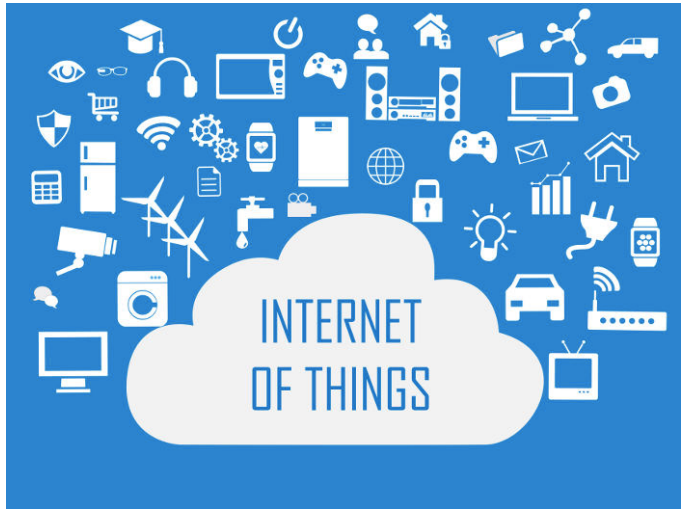


Mobile Internet

Mobile Internet Anywhere

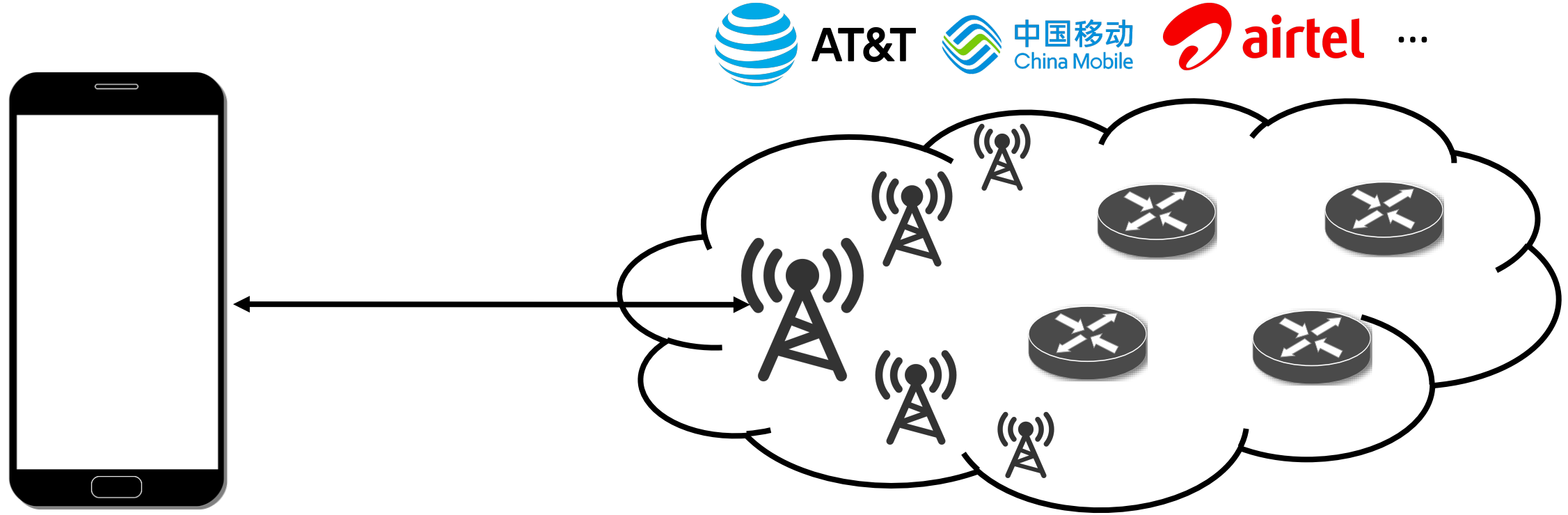


More than Mobile Internet …



Mobile Networked Systems

- The only large-scale wireless network infrastructure for the massive market



Mobile device
(user equipment)

Cellular network Infrastructure
(radio + core)

Towards Better App Performance & User Experience over Mobile Networks

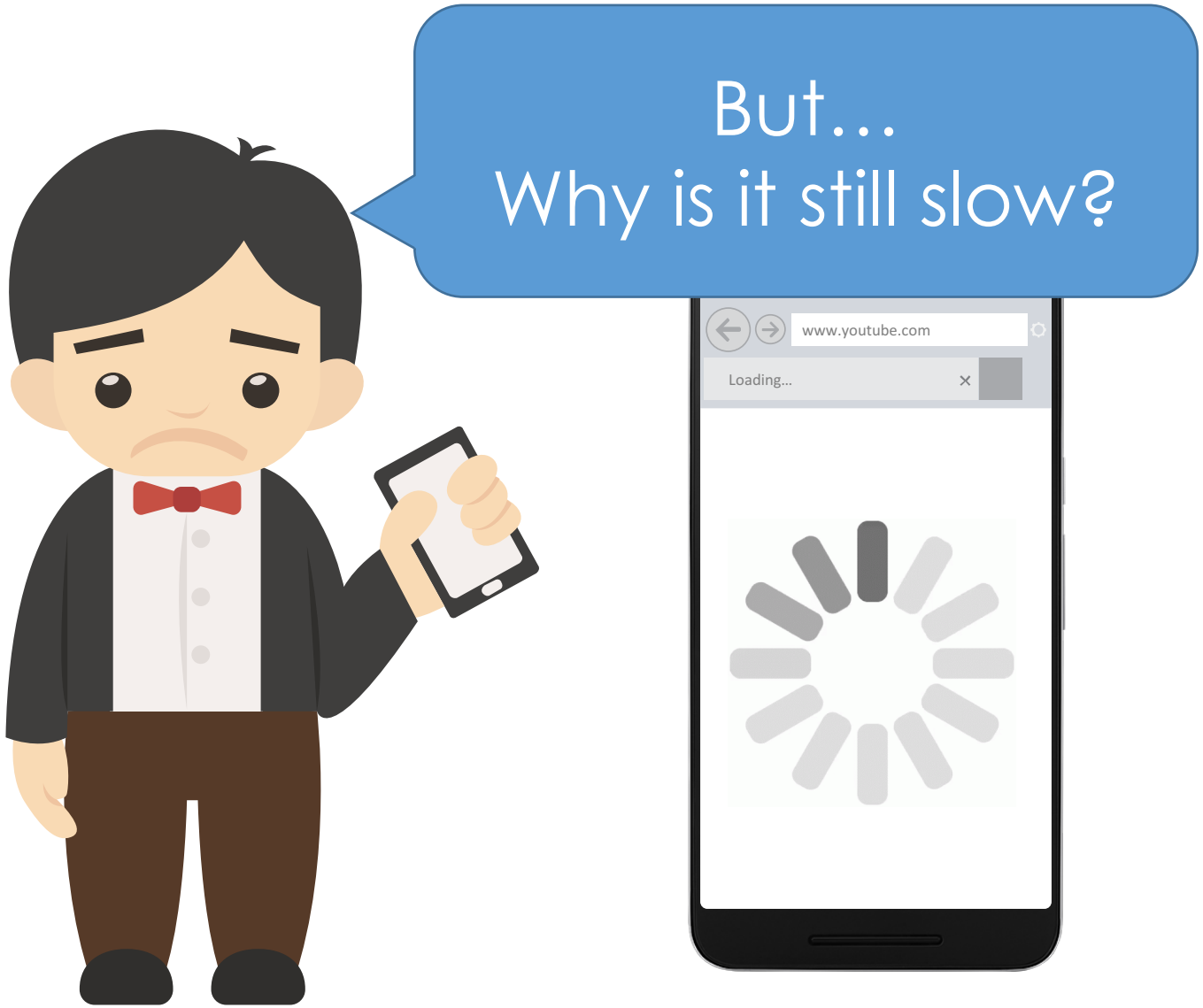
Our Goal

Performance, Efficiency, Reliability …

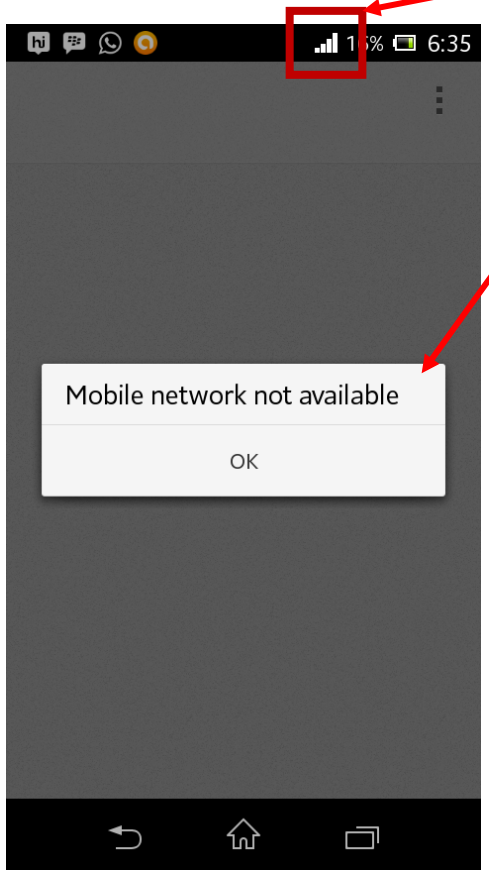
However,


5 Signal bars.
Fast network speed.
Awesome!
Advanced Pro
LTE
10
5
20
1
50
0
100+
3.11
Megabits per second
Testing download...

However,

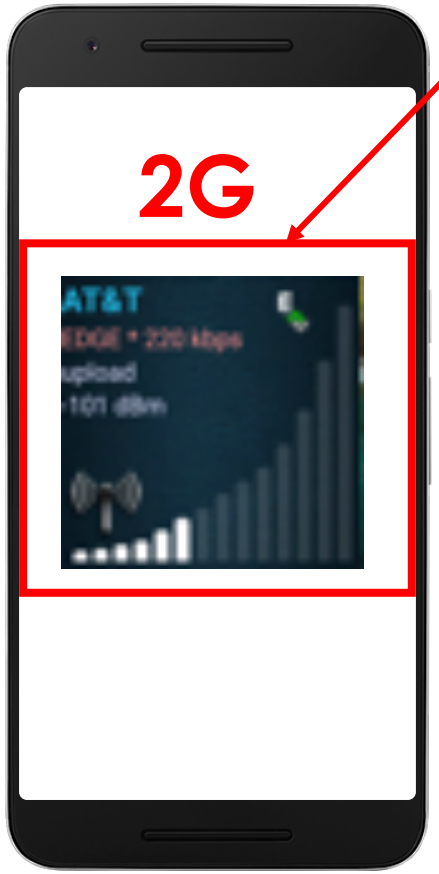


Many Examples in Our Daily Life



Good radio quality,
Why no data?

Many Examples in Our Daily Life



Why 2G, not 4G when 4G available?

Many Examples in Our Daily Life

- Web: 1s-10s seconds
- Video: slow start, stall
- VR/AR: slow response
- Call: drops or fails
- … …

We Need to Know

- What
- Why
- How

So that, We Can

- Unveil and understand real problems
  - Identify real problems such as poor performance, degrades, failures, …
  - Verify them and assess their impacts
  - Reason about and understand their root causes

- Improve performance, efficiency, reliability
  - Gain solution insights
  - Design, implement and validate solutions

- Over **real** mobile networked system

We Like Real Things, But

- Many choose model-simulation-based work
  - Assumptions → formulation → system model → theoretical analysis → algorithm → simulation
- The good
  - Fundamentals(theoretical bounds and properties)
  - Fit for module designs (e.g., channel estimation)
- The bad
  - Simplistic and even artificial
  - Practical factors not considered in the evaluation
  - Solutions not deployable (not standard compatible, too many changes required at heavy cost)
  - …

In Many Cases, We Choose Simulation

- Only because we can't do it in practice
  - No access to real mobile network operations
  - Can't obtain operation data from carriers
  - Don't know what interfaces exposed to us
  - Complexity in handling practical factors
  - …

This Tutorial: From Simulation to Practice

- Introduce an approach to know

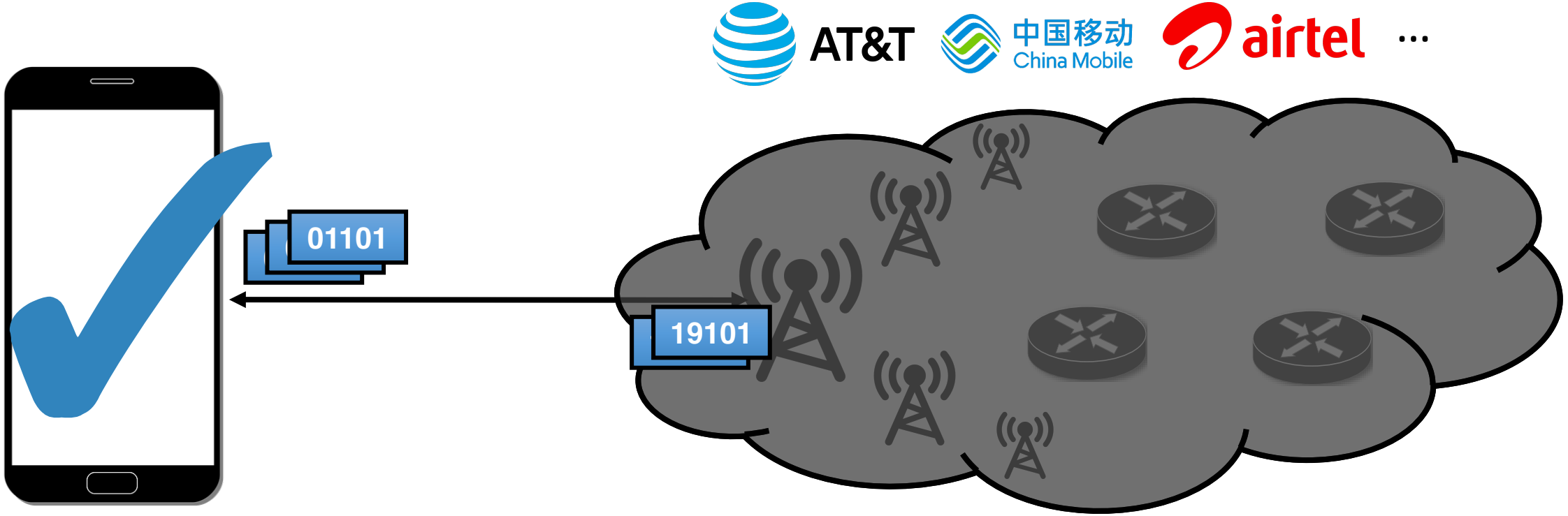
What

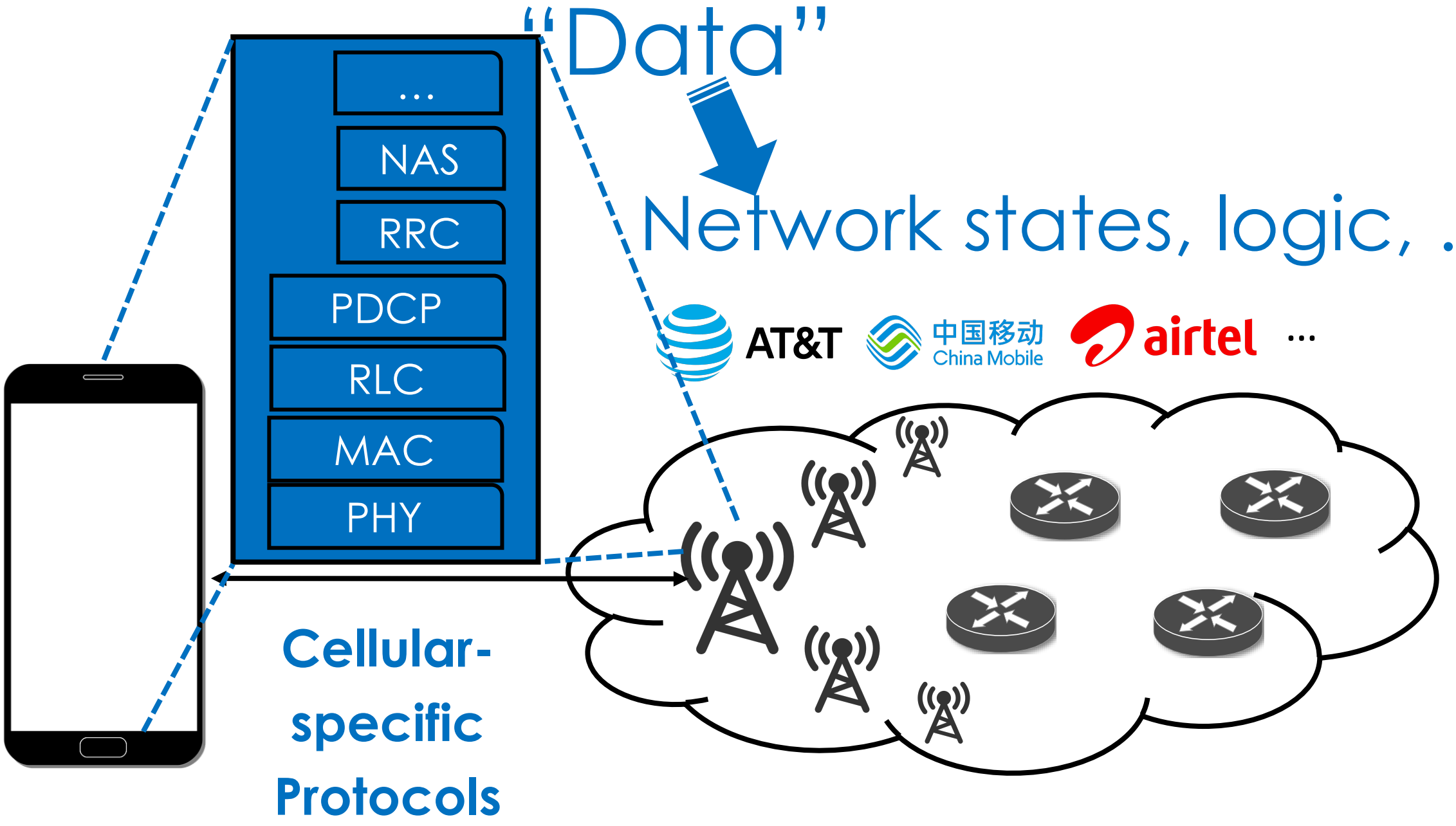
Why

How

This Approach

- In-Device (not at network)
- Data-driven (msgs btw device-network)




"Data"
Network states, logic, …
…
NAS
RRC
PDCP
RLC
MAC
PHY
AT&T
中国移动
China Mobile
airtel
…
Cellular-specific Protocols

This Tutorial: From Simulation to Practice

- Introduce an approach to know what, why & how

  - Via MobileInsight [Mobicom'16]
  - Monitor and analyze network operations on your smartphones
  - Ready for everyone: no operator assistance needed, no special hardware/instrument required

This Tutorial: From Simulation to Practice

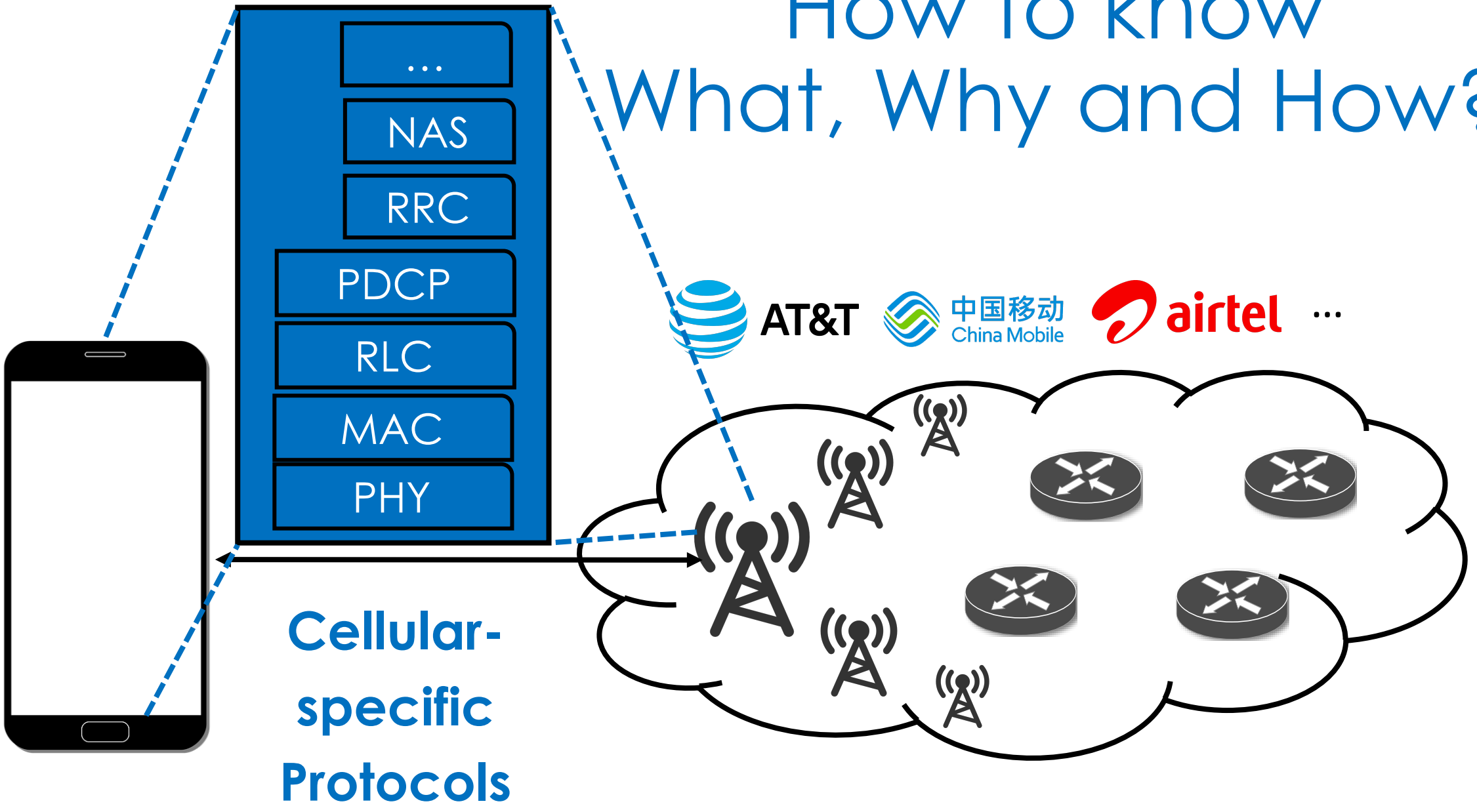
- Introduce an approach to know what, why & how
  - Via MobileInsight [Mobicom'16]

- Use this approach to unveil, verify and solve real problems
  - Case study: analytical methods and effectiveness
  - Case study: performance enhancement

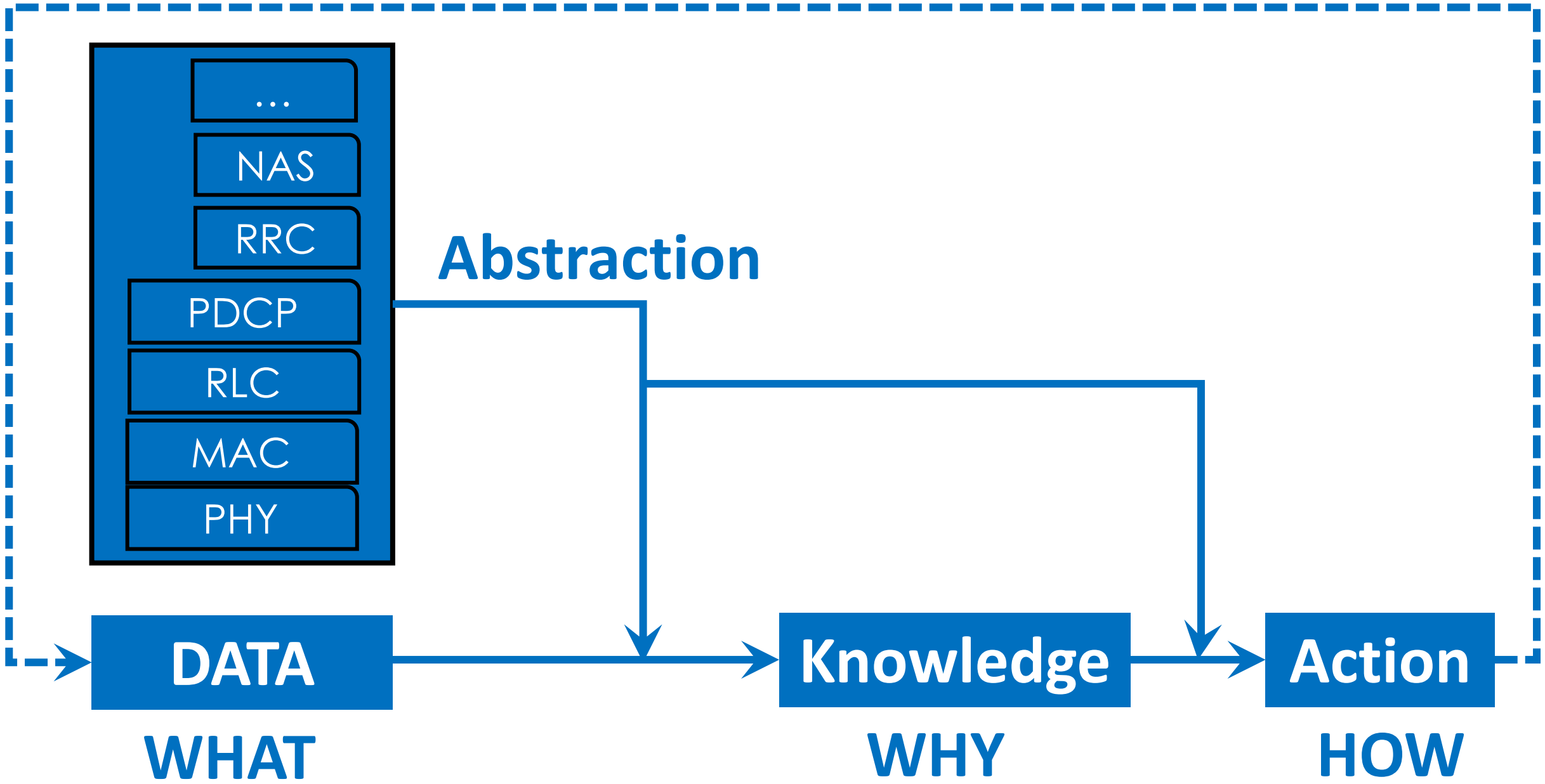
This Tutorial: Agenda

- ✓ Introduction
- ✓ Tutorial overview
- ⬇ **MobileInsight: first look**
4. Primer on cellular protocols
5. MobileInsight: second look
6. Research opportunities and examples
7. Advanced topics
8. Closing remarks

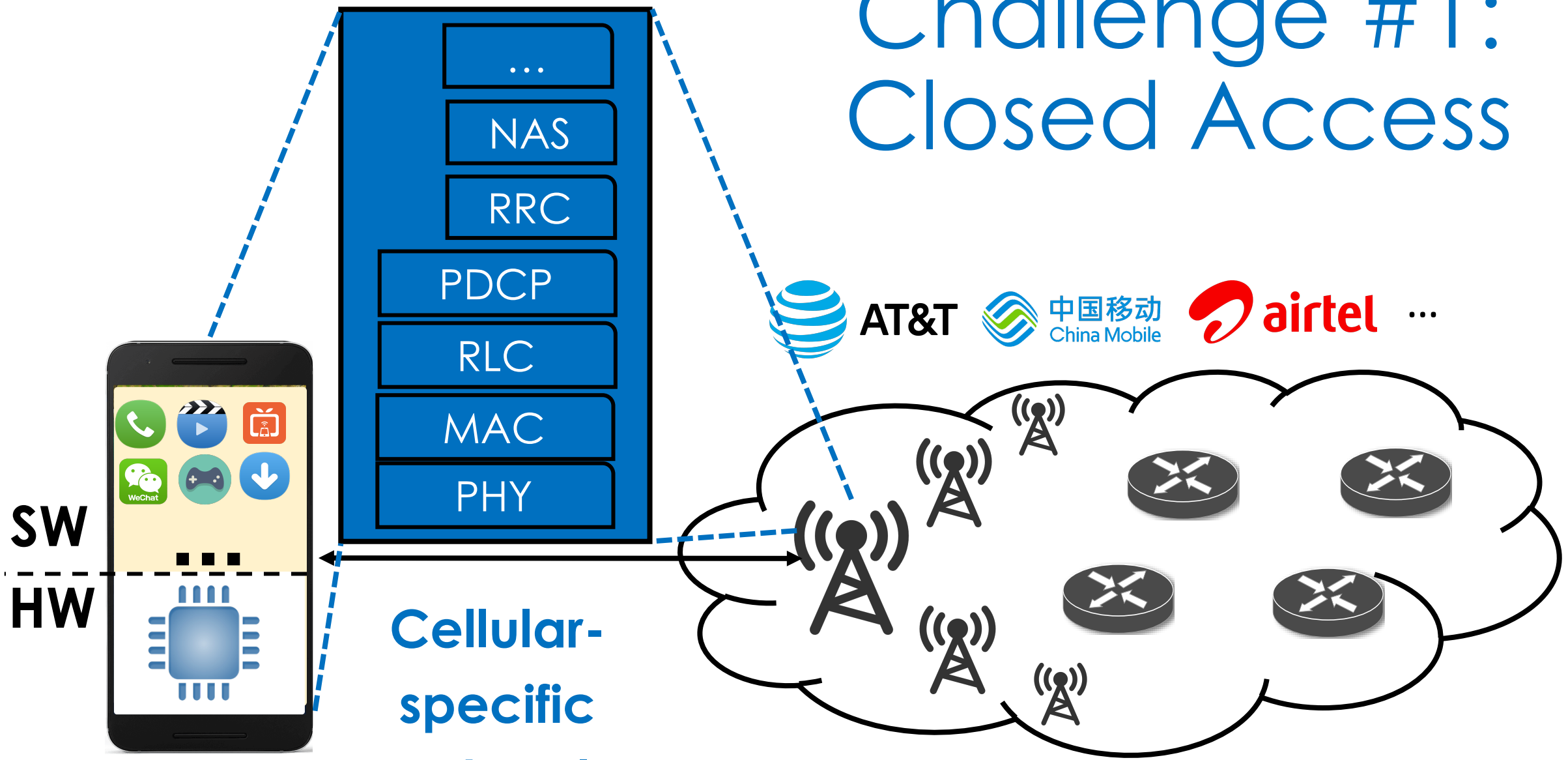
How to know What, Why and How?



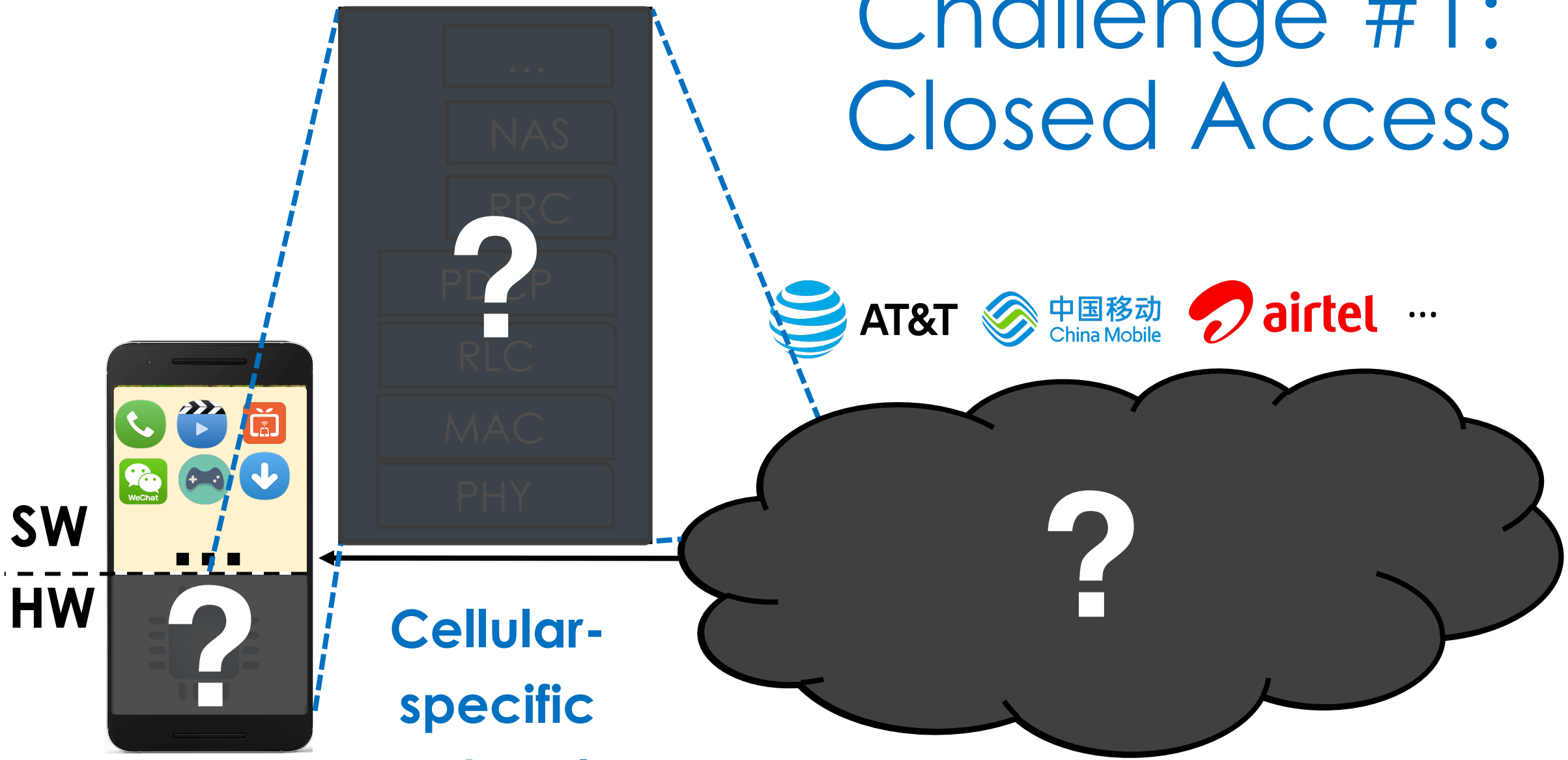
Approach: Data-Driven Learning Cycle



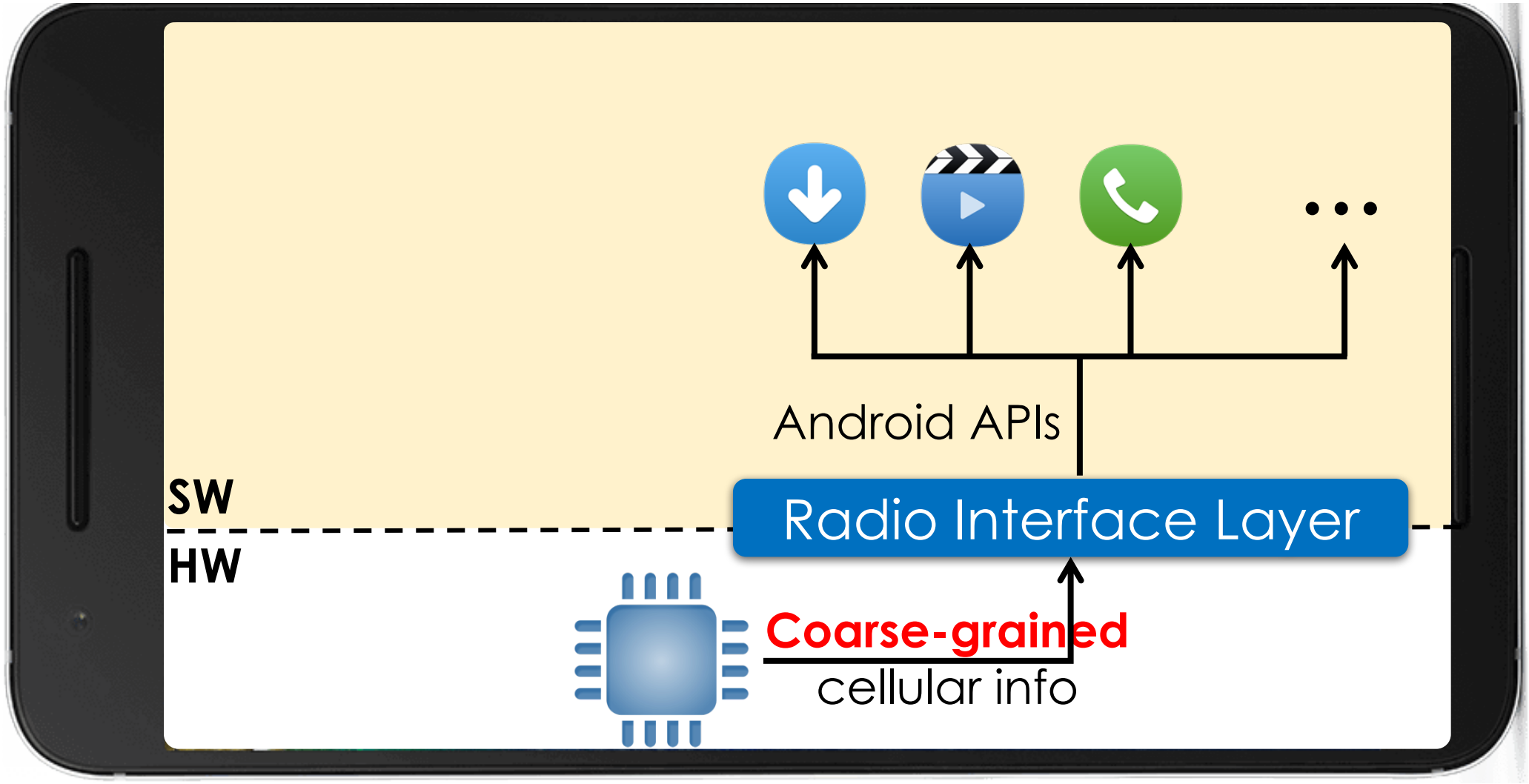
Challenge #1: Closed Access



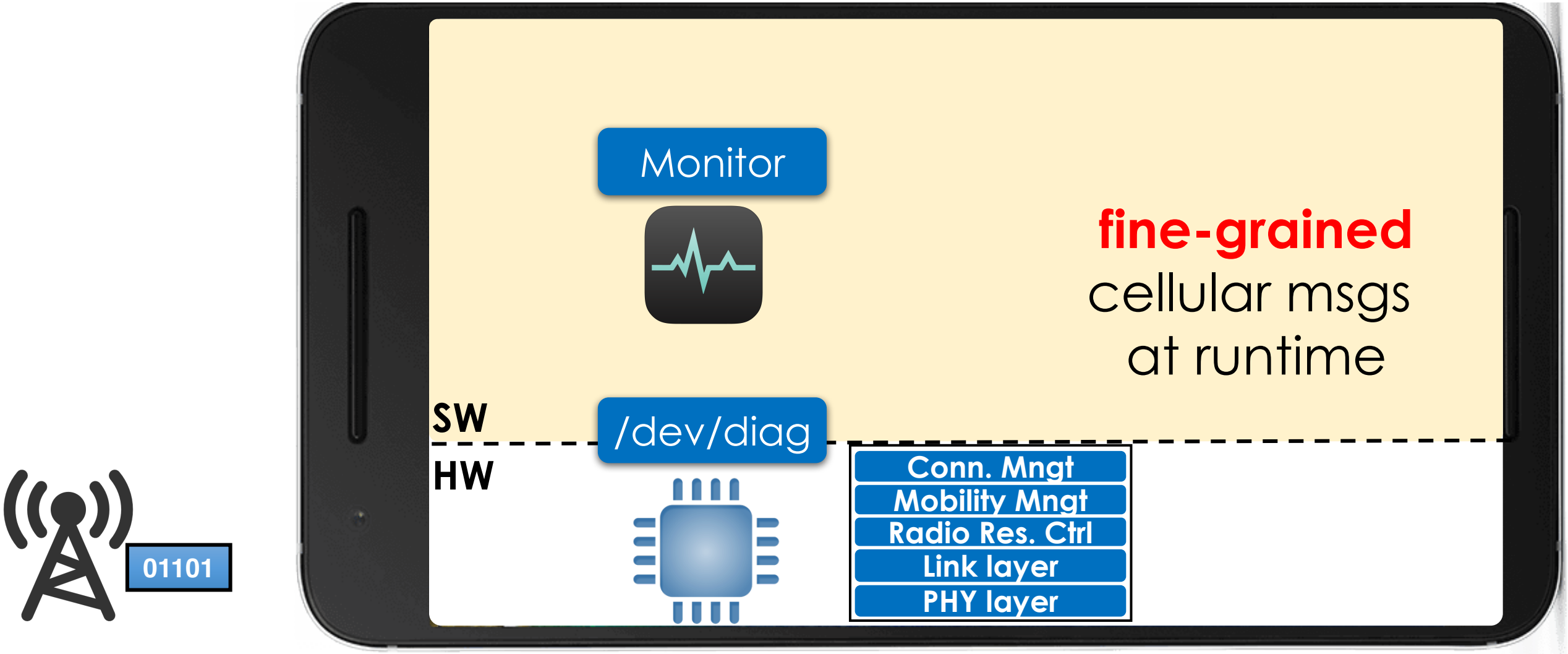
Challenge #1: Closed Access



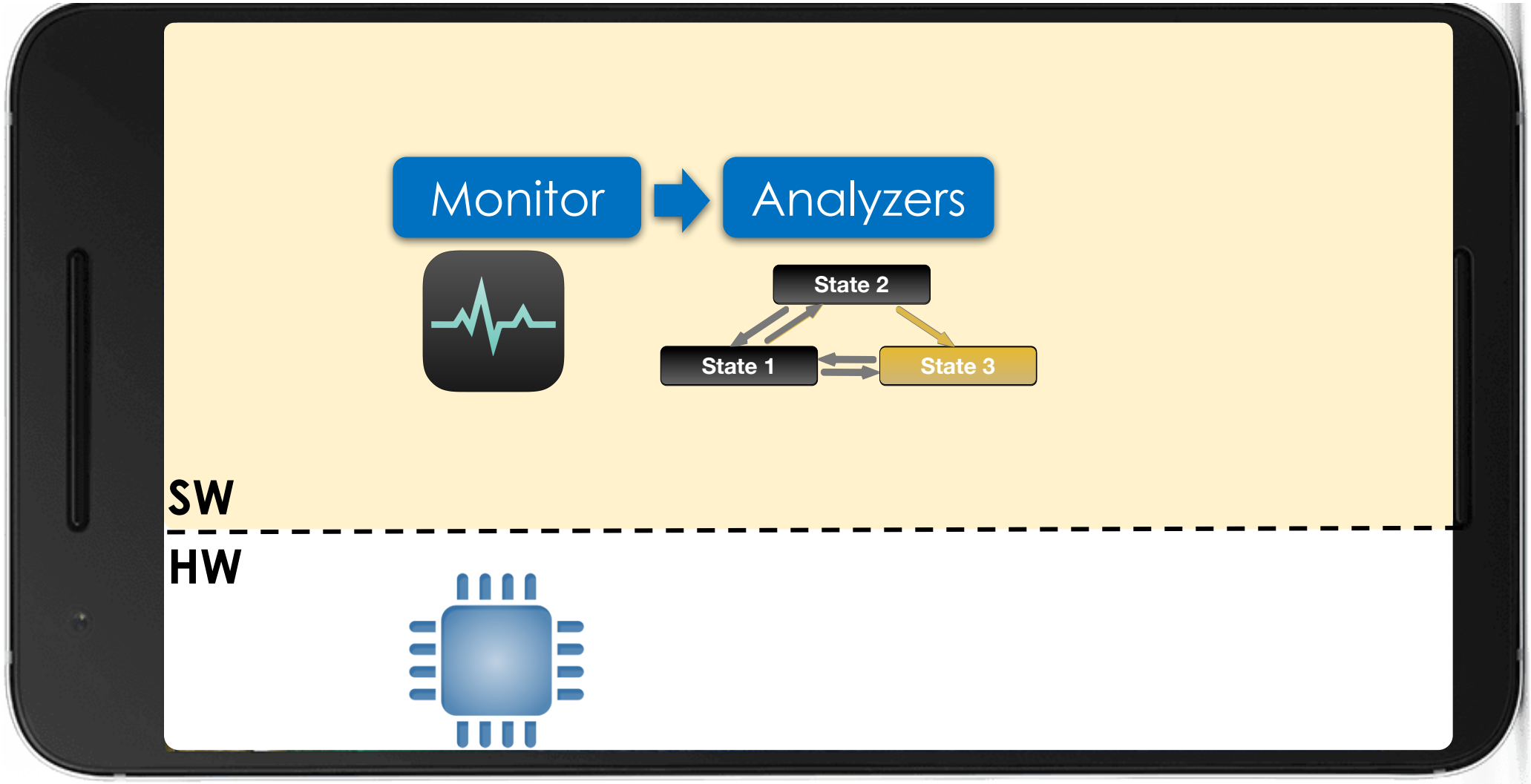
No Ordinary Interface @ Device



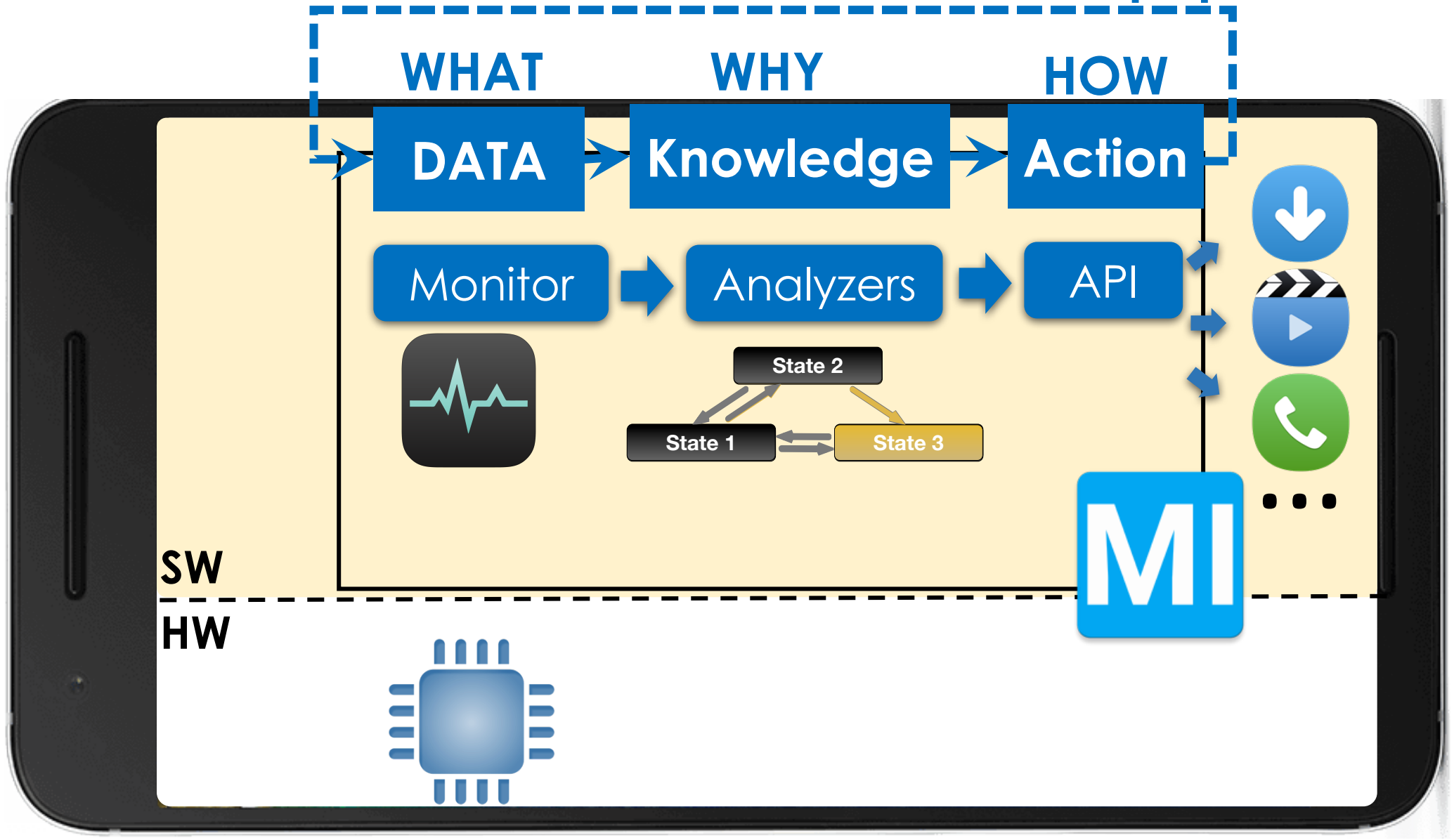
Open Data Access via /dev/diag



Build Protocol Analytics



Expose Inferred States to Apps

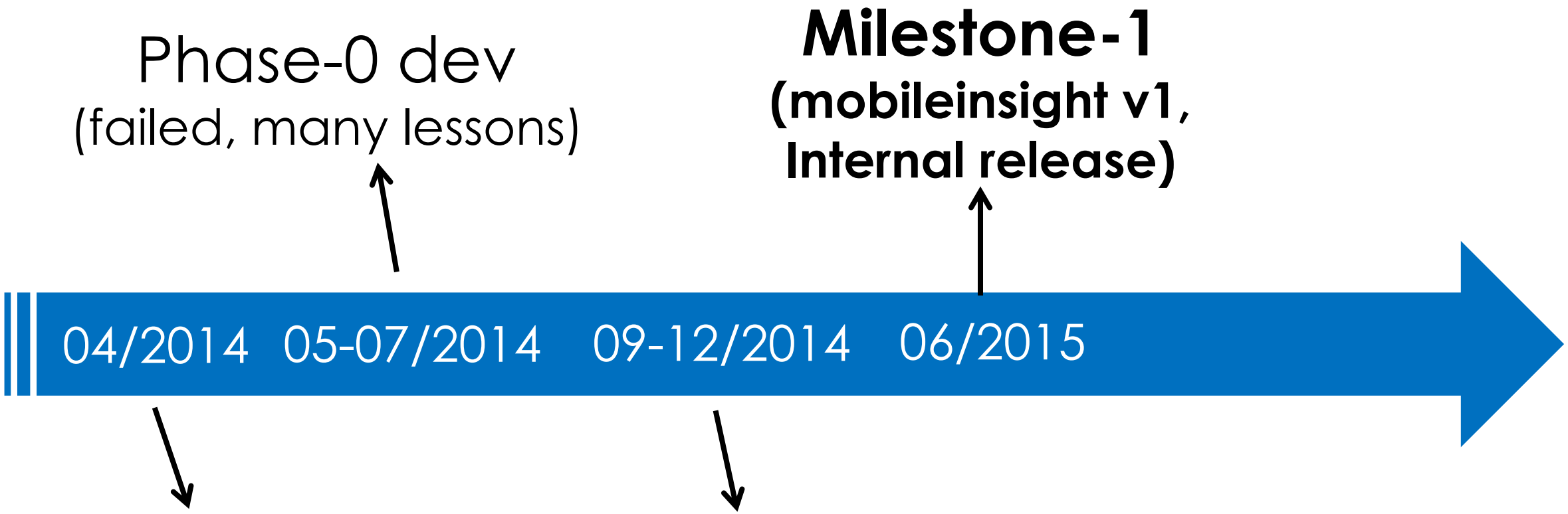


MobileInsight: Many Benefits

	Full msg coverage	Fine grained	Analysis	At scale	In-phone
MI	✔	✔	✔	✔	✔
Android APIs	✘	✘	✘	✔	✔
External Tools (e.g., QXDM)	✔	✔	✘	✘	✘
Operator-side cellular analytics	✔	✔	✔	✘	✘

MobileInsight Timeline

Website: http://www.mobileinsight.net/
Github: https://github.com/mobile-insight



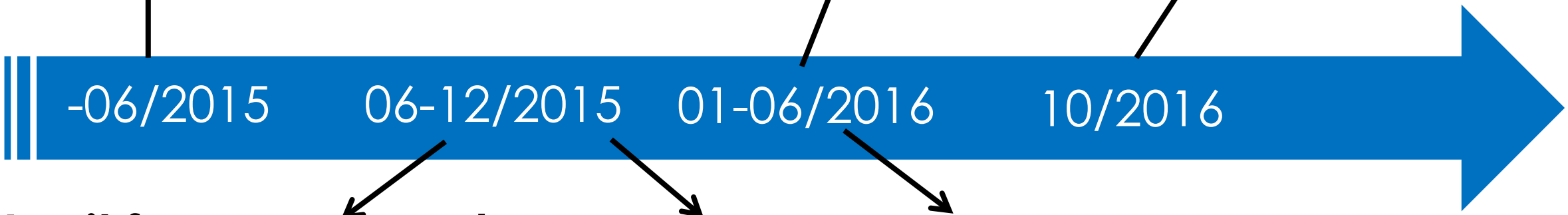
MobileInsight Timeline

Website: http://www.mobileinsight.net/
Github: https://github.com/mobile-insight

Milestone-1
(mobileinsight v1, Internal release)

Milestone-2
(mobileinsight v2, First public release)

Mobicom'16 Best Community Paper Award



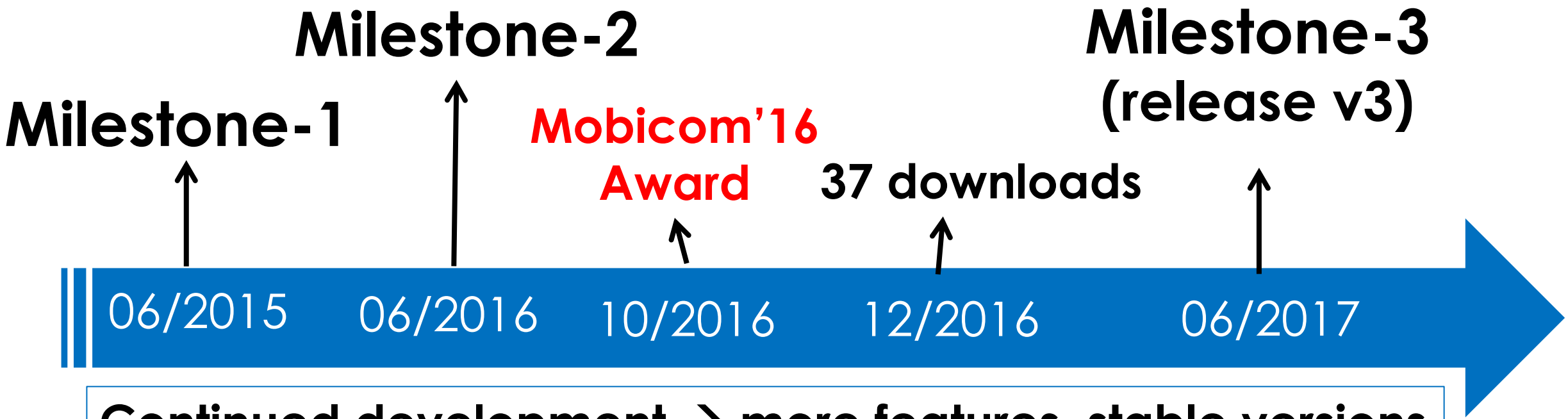
Use it for our research
(NSDI'16, SIGMETRICS'16)
Continued development
→ a stable version

Submitted to Mobis'16
X

Continued dev
→ More features
Submitted to
MobiCom'16 (03/16)

MobileInsight Timeline

Website: http://www.mobileinsight.net/
Github: https://github.com/mobile-insight



Continued development → more features, stable versions,

+ technical support, help others to do research of their interests

MobileInsight Timeline

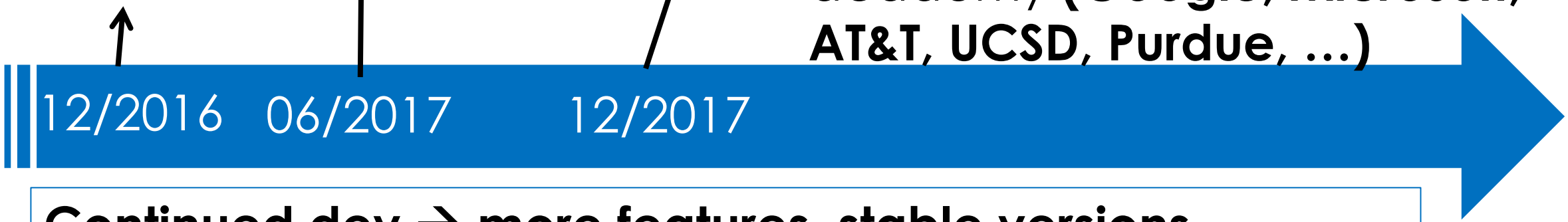
Website: http://www.mobileinsight.net/
Github: https://github.com/mobile-insight

Milestone-3 (release v3)

37 downloads

V3.3 release, 170+ downloads

- **3rd-party** developers
- **10+ projects** from industry& academy **(Google, Microsoft, AT&T, UCSD, Purdue, …)**



Continued dev → more features, stable versions,

+ technical support, help others to do research of their interests

Where is MobileInsight heading to?

- **Community tool in mobile network research**
  - ***For*** the community, ***by*** the community
- **Open-source codes** (github)
  - Mobile (Android apk)
  - Core (offline analyzer)
  - Libs, python-for-android, dev
- **Open datasets** (raw: 400+GB)
- **Open experimentation testbed** (release soon)

What MobileInsight Can Do For You?

- ✓ Wide coverage of protocols/msgs
  - Full set of 4G/3G control-plane protocols
  - Most 4G data-plane protocols + partial 3G/2G support
  - 3GPP releases 7-12 + release 13 - 14 (partially)
- ✓ A variety of devices supported
  - 25 + phone models
  - Android (iOS ongoing)
  - Qualcomm Snapdragon, MediaTek (partially)
- ✓ Responsive and effective
  - Processing time within 0.8ms (99+%)
  - Effective in analyzing handoff (mis)configurations, security loopholes, failures/degrades, …
- ✓ Acceptable overhead
  - CPU: 1-3% @S5,6P, RAM: <30 MB, Power: 11-58mw; (on some models)

Demo #1: Getting Started

- For beginners (mobile users)
- For rooted android phones

- Step 1: Download & install MobileInsight
- Step 2: First run
  - Setting
  - NetLogger
  - Log browser

apk: http://www.mobileinsight.net/download.html

nt

Beg

Demo #1: Getting Started

- For beginners (mobile users)
- For rooted android phones

- Step 1: Download & install MobileInisght
- Step 2: First run

- Encourage "data sharing"
- Log Brower: view, filter & search
- Advanced topics: your own plugin, offline browser

Next, How to Use it for Research

Use this approach to unveil, verify and solve real problems

The Key:
What cellular-specific information can be exposed to smartphone?

Answer: 3GPP + Chipset debug info

- Procedures: message flows
- Messages
- Message fields

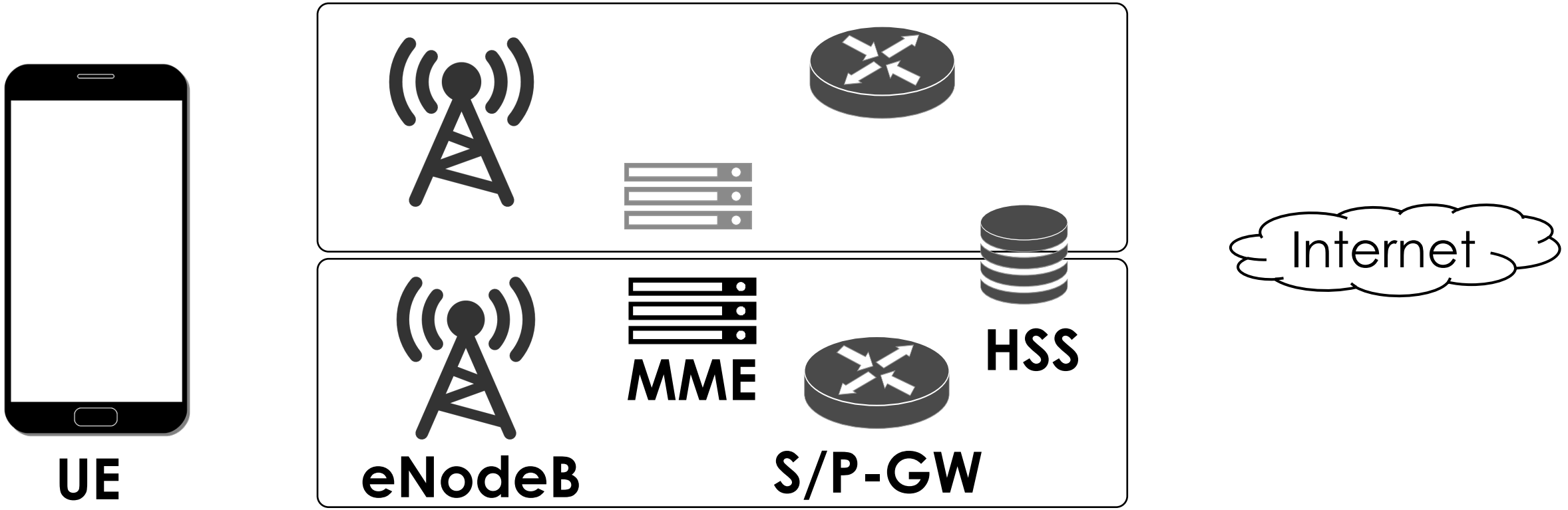
This Tutorial: Agenda

- ✓ Introduction
- ✓ Tutorial overview
- ✓ MobileInsight: first look
- ⬇ Primer on cellular protocols

5. MobileInsight: second look
6. Research opportunities and examples
7. Advanced topics
8. Closing remarks

Mobile Network Architecture

Use 4G LTE as an example



UE: user equipment
eNodeB: base station
MME: mobility management entity
S-GW: serving gateway
P-GW: PDN gateway
HSS: home subscriber server

Three-Plane Operations

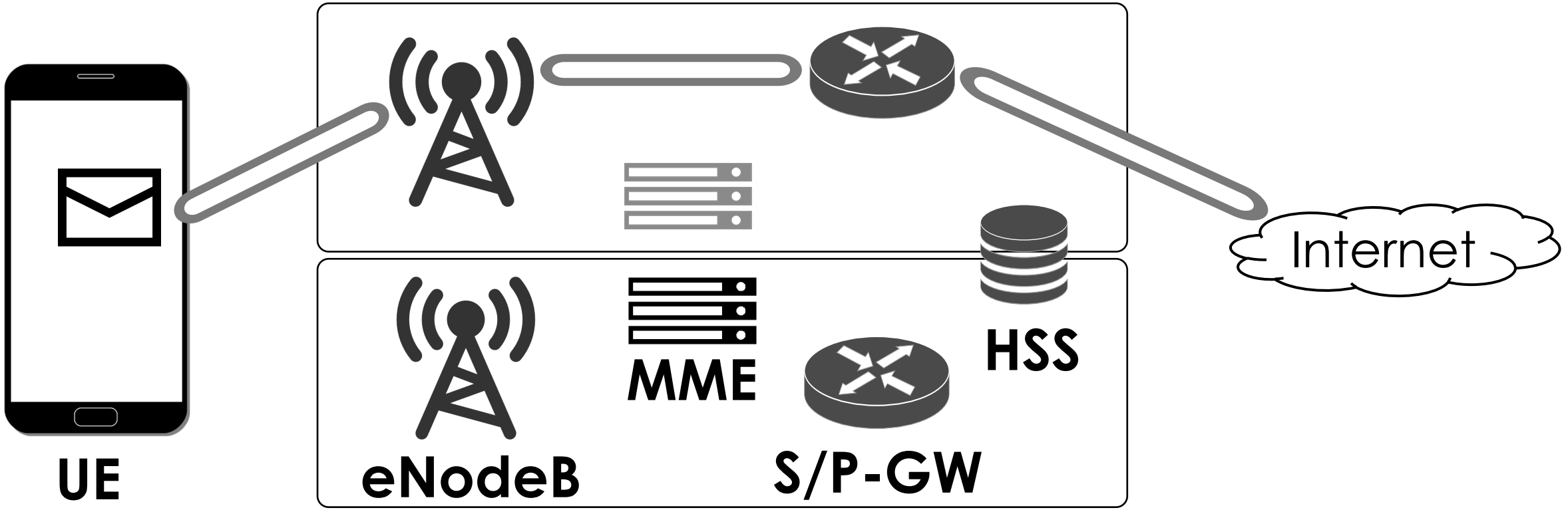
Three planes in operation in parallel:

- **Data plane (also called User plane)**: user content delivery (data, voice, sms, ...)
- **Control plane**: signaling functions
  - Radio resource control, mobility, connectivity
- **Management plane**: configurations, monitoring

Data-Plane Operations

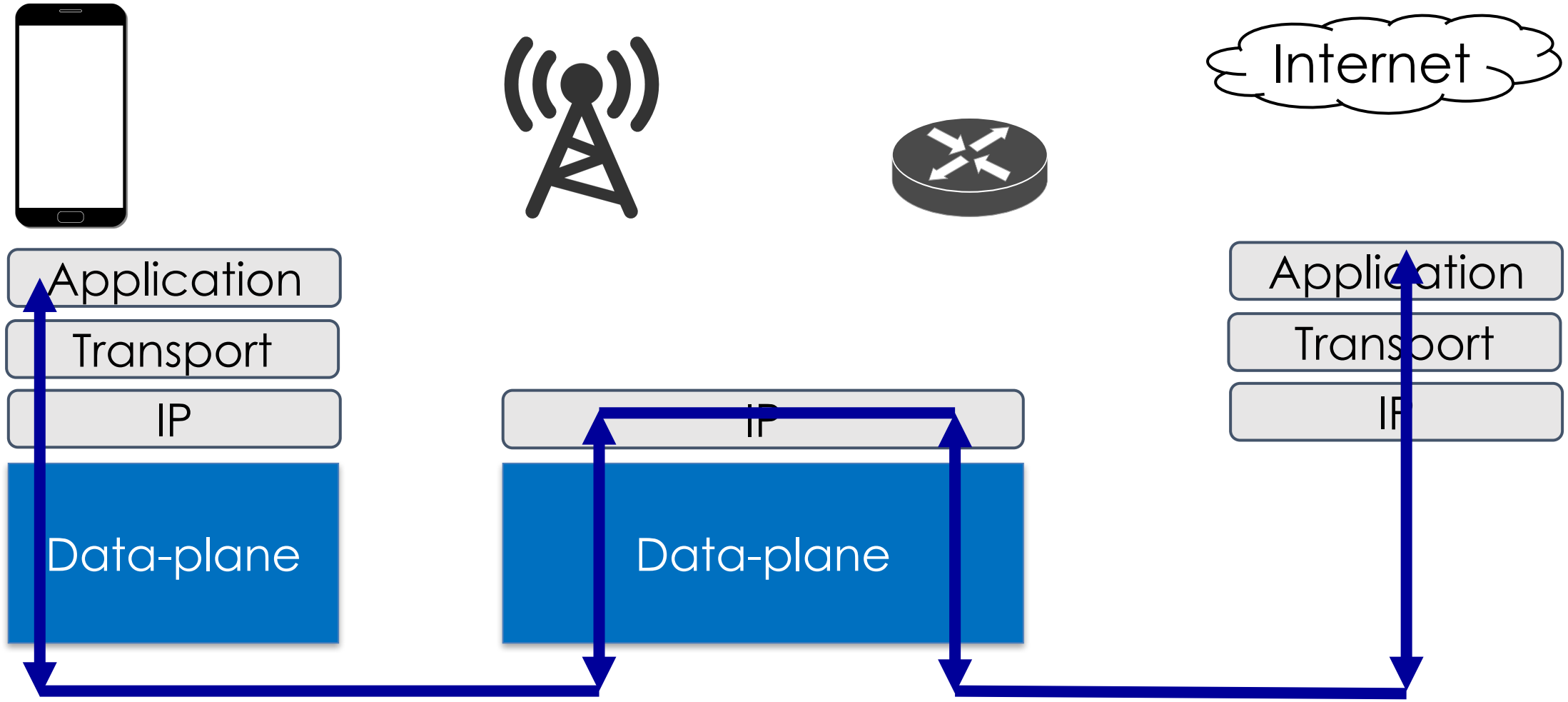
Data-plane

Use 4G LTE as an example

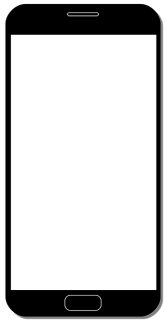


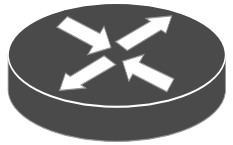
UE: user equipment
eNodeB: base station
MME: mobility management entity
S-GW: serving gateway
P-GW: PDN gateway
HSS: home subscriber server

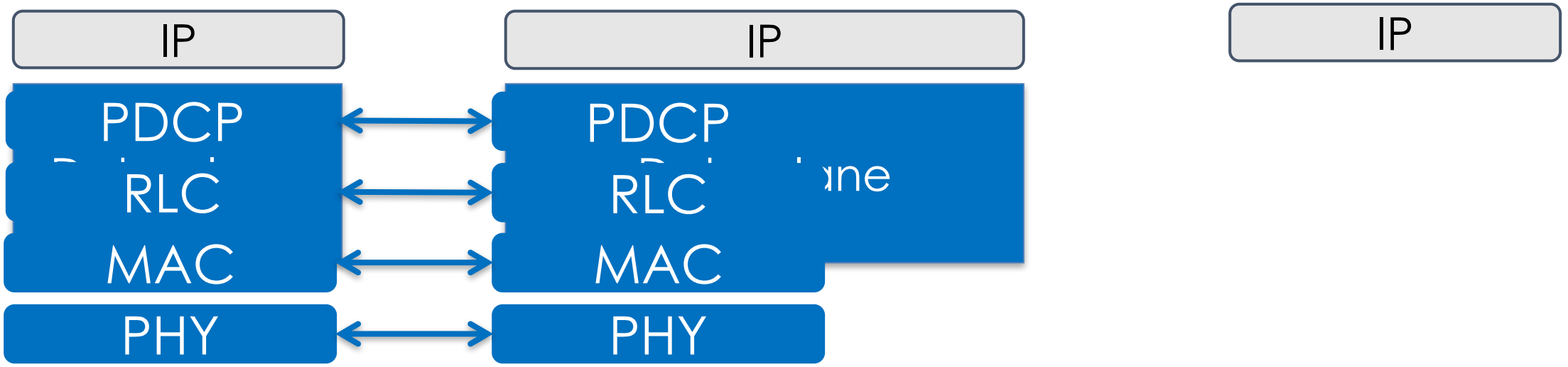
Data-Plane Protocols



Data-Plane Protocols

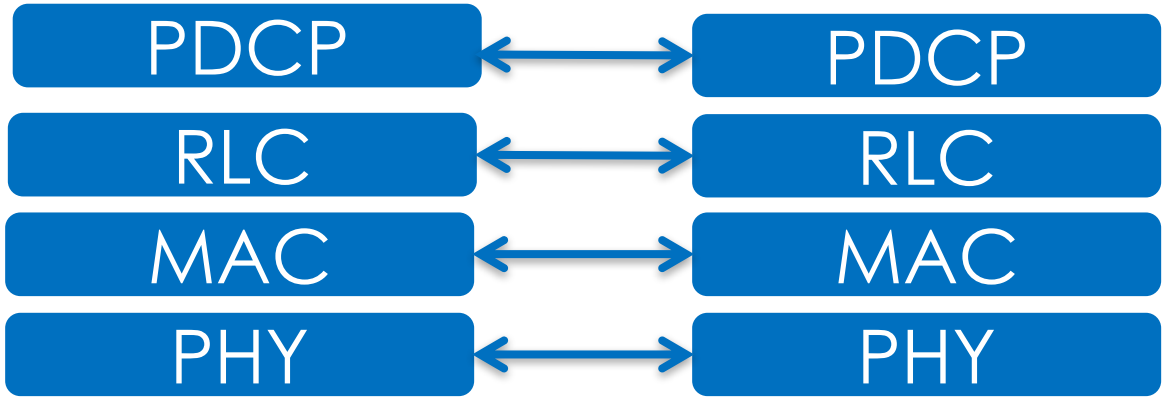






Below IP: L1/L2 Protocols

- **Packet Data Convergence Protocol (PDCP)** – header compression, radio encryption
- **Radio Link Control (RLC)** – Readies packets to be transferred over the air interface
- **Medium Access Control (MAC)** – Multiplexing, QoS
- **Physical (PHY)** – preamble, sync, modulation and coding scheme, …



Rich Information Below IP

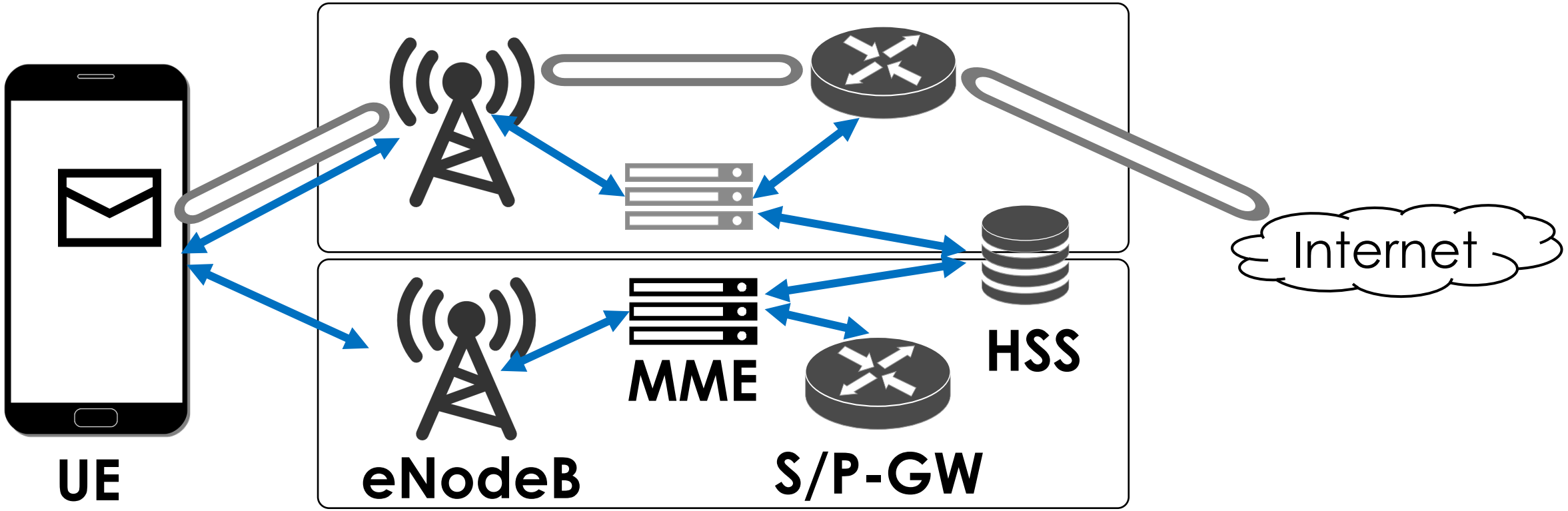
- Many messages, please refer to 3GPP TS36.323, TS36.322, TS36.321, TS36.211, TS36.212, TS36.213, TS36.214
- PDCP, e.g.,
  - How many packets dropped? number of data/control bytes, number of RBs
- RLC, e.g.,
  - which mode used?
- MAC, e.g.,
  - How many bytes sent? When (at which subframe) ?
- PHY, e.g,.
  - Radio measurement of serving and neighbor cells at idle or connected state
  - Power control
  - Physical channel indications
  - Error rate

Later, we can see them in MobileInsight (Demo #2)

Control-Plane Protocols

Data-plane ↔ Control-plane

Use 4G LTE as an example

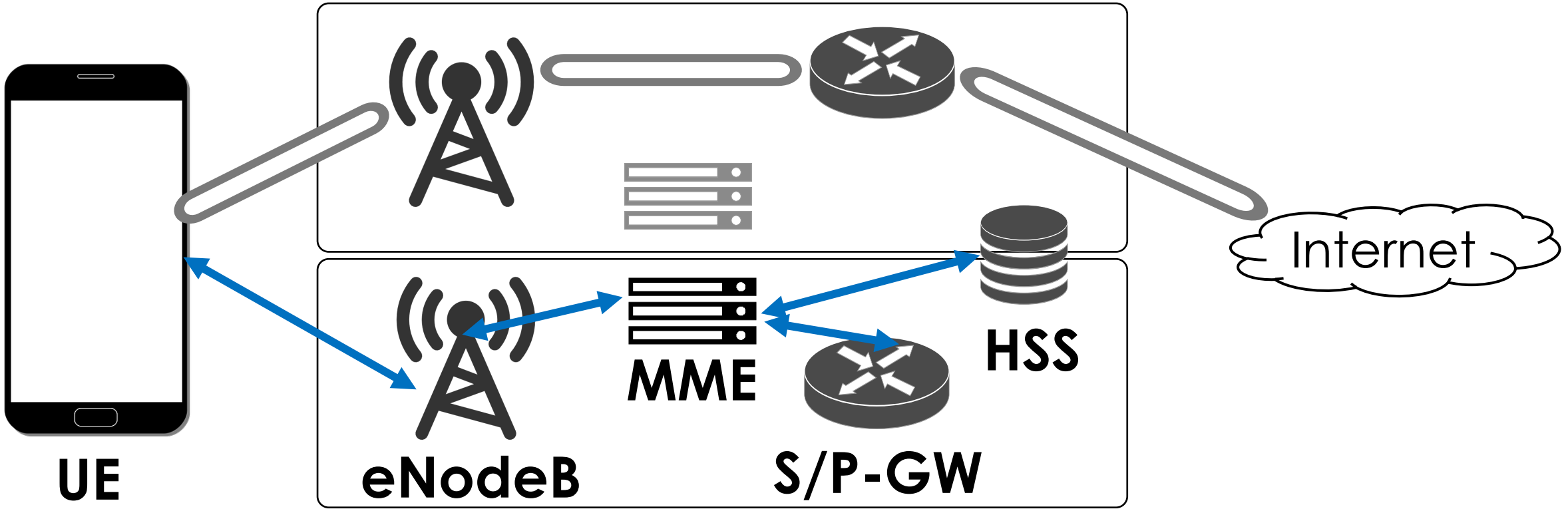


UE: user equipment
eNodeB: base station
MME: mobility management entity
S-GW: serving gateway
P-GW: PDN gateway
HSS: home subscriber server

Control-Plane Protocols

Data-plane ↔ Control-plane

Use 4G LTE as an example



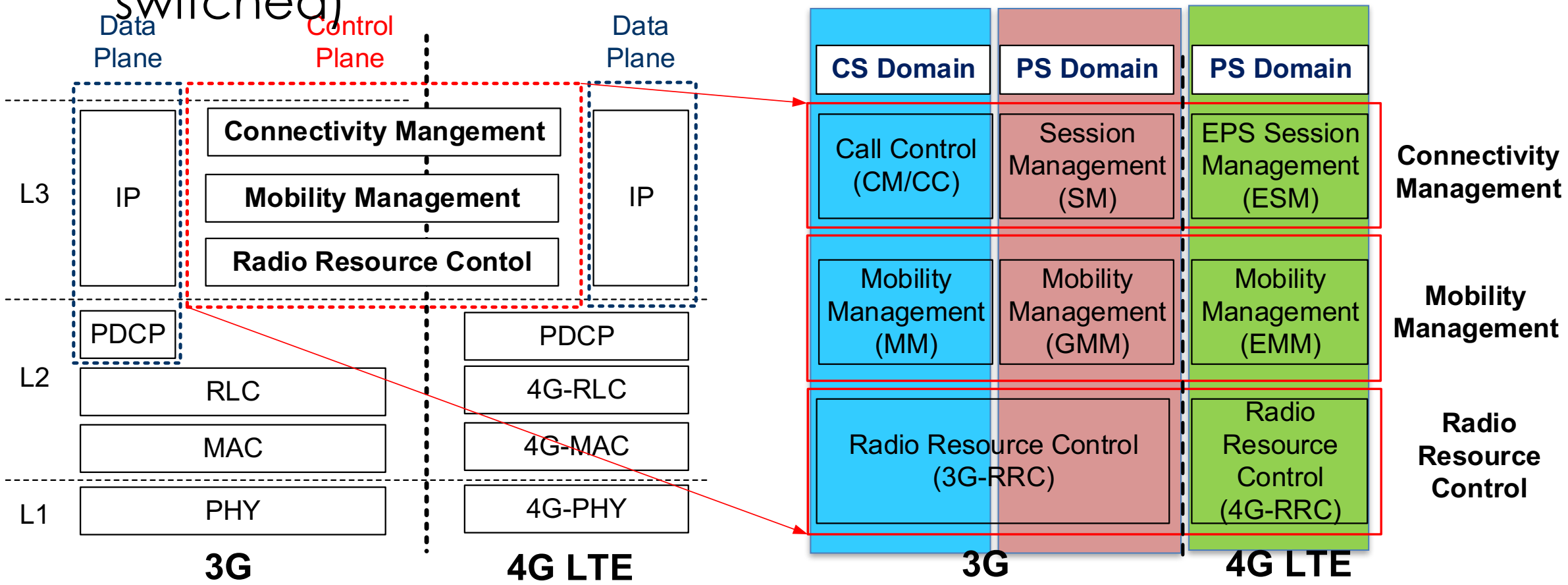
Connectivity Management

Mobility Management (MM)

Radio Resource Control (RRC)

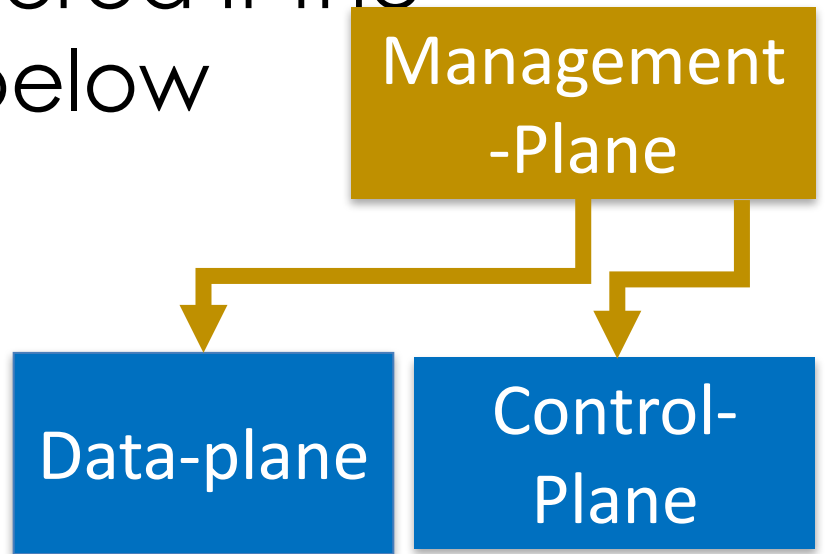
Protocol Variants

- Multiple releases (Release 8 – Release 14)
- Hybrid system (2G/2.5G/3G/3.5G/4G/4.5G/5G)
- Separated domains: data (packet-switched), voice (circuit-switched)



Management-Plane

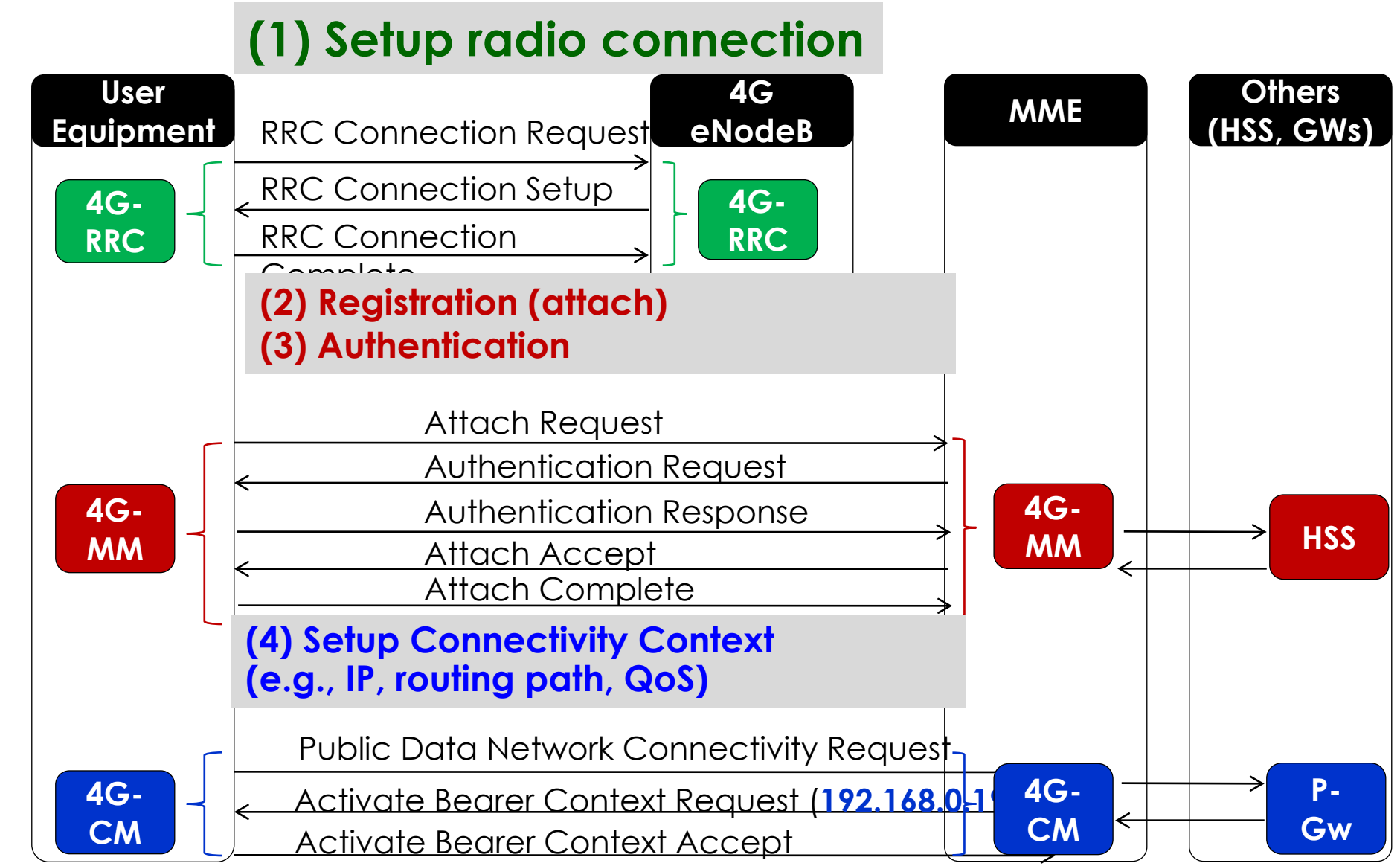
- Many types of configurations, e.g.,
  - Timers: RRC setup timer (T300)
  - Counts: Maximum of retries if RRC setup fails
  - Priority: Voice (VoLTE) has highest priority (1) for signaling, normal data uses low priority (6-9)
  - Thresholds: Measurement is triggered if the current serving radio strength is below thresholds



Procedure: Message Flows

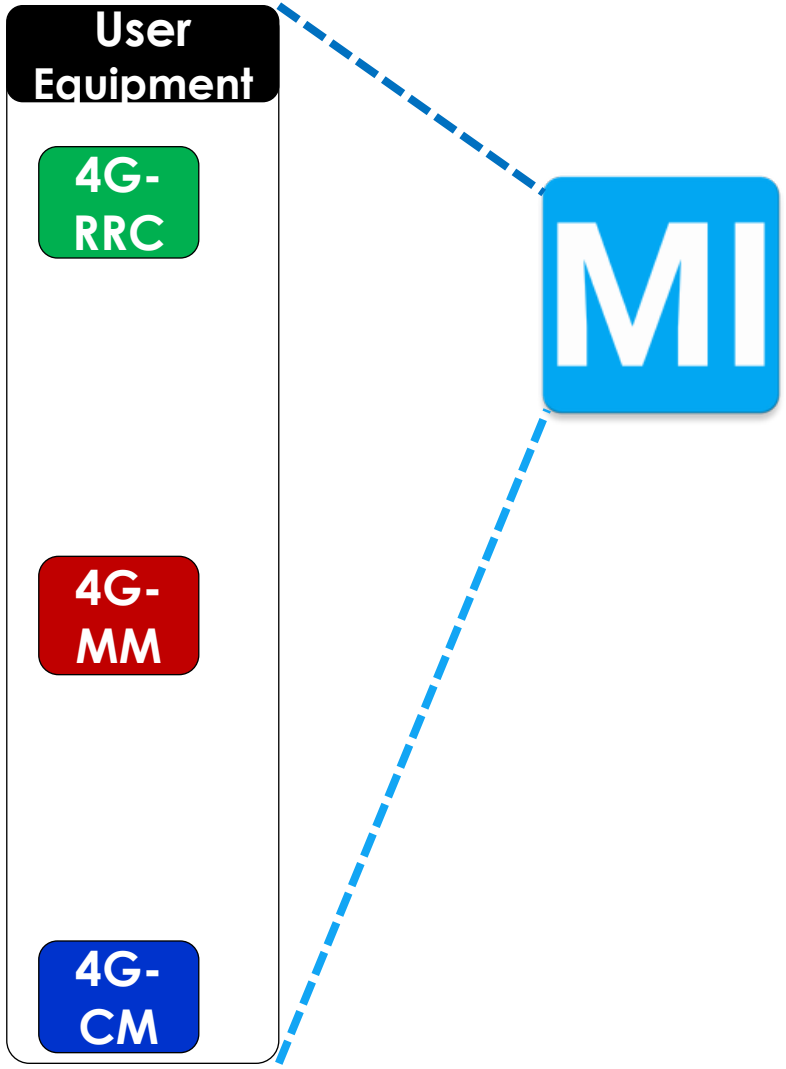
- Management-plane: configuration in advance
- Control-plane: signaling functions first
  - Establish states at network elements
  - E.g., data connectivity setup
  - E.g., mobility (handoff, cell-reselection)
- Data-plane: data transfer once ready

Example: Establish Data Service in 4G



PDN: Public Data Network EPS: Evolved Packet System

From the Device-side View



MI

- Messages exchanged between UE and network
- Message sequence → protocol, states
- Message fields → parameters
- →runtime inference of network dynamics and logic

Demo #2: Collect Logs of Your Interest

- For beginners (mobile users)
- For rooted android phones

- Run "NetLogger" in certain test scenarios
  - RRC connection: turn off and on data, → web
  - Cell configurations: manual switch from LTE to 3G → system information blocks
  - Call procedure: make a phone call
  - …
- Browse logs collected and locate fields of interests

5 Minute Break

This Tutorial: Agenda

- ✓ Introduction
- ✓ Tutorial overview
- ✓ MobileInsight: first look
- ✓ Primer on cellular protocols
- ✓ MobileInsight: second look
- ⬇ Research opportunities and examples

7. Advanced topics
8. Closing remarks

Now, How to Use it for Research

Use this approach to unveil, verify and solve real problems

Open Research Opportunities

Unveil & understand real problems

Sample projects:

- Network diagnosis
- Network verification
- Mobile big data analytics
- …

Improve performance , efficiency, reliability

Sample projects:

- Cross-layer optimization
- Security enhancement
- Protocol optimization
- …

Selective Publications

Unveil & understand real problems

Improve performance , efficiency, reliability

SIGMETRICS'16

Instability in Distributed Mobility Managem

Revisiting Configuration Management in 3G/4G Mobile Ne

Yuanjie Li†, Haotian Deng‡, Jiayao Li†, Chunyi Peng‡, Songwu L

†University of California, Los Angeles, *The Ohio State University

yuanjie.li@cs.ucla.edu, deng.264@buckeyemail.osu.edu, likayo@uc

chunyi@cse.ohio-state.edu, slu@cs.ucla.edu

NSDI'16

iCellular: Device-Customized Cellular Network Access on Commodity Smartphones

MobiCom'17

A Control-Plane Perspective on Reducing

Access Latency

Accelerating Mobile Web Loading Using Cellular Link Information

Shilin Zhu
University of
Wisconsin-Madison

Automotive UI

Investigating Remote Driving over the LTE Network

Ruilin Liu[1], Daehan Kwak[2], Srinivas Devarakonda[1], Kostas Bekris[1], and Liviu Iftode[1]
[1]Department of Computer Science, Rutgers University, USA
[2]Department of Computer Science, Kean University, USA
[1]{rl475, skd70, kostas.bekris, iftode}@cs.rutgers.edu, [2]dkwak@kean.edu

Globecom'17

Discover Your Competition in LTE: Client-Based Passive Data Rate Prediction by Machine Learning

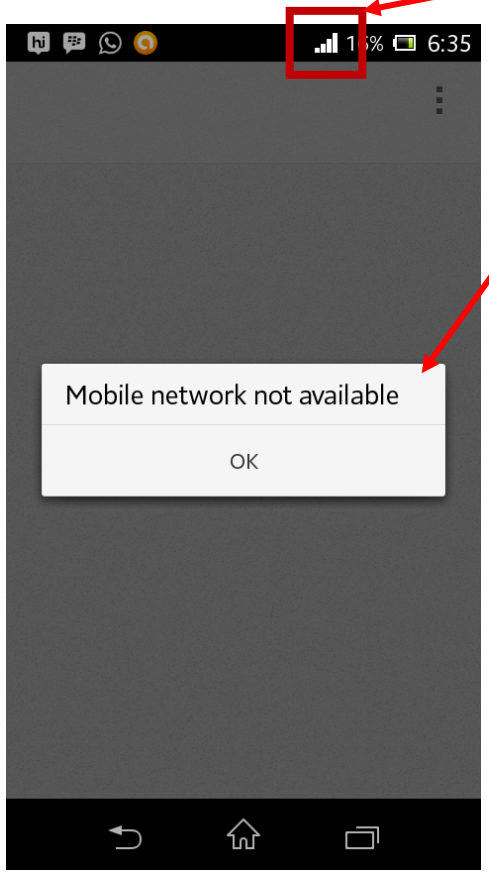
Robert Falkenberg, Karsten Heimann and Christian Wietfeld
Communication Networks Institute
TU Dortmund University
44227 Dortmund, Germany
Email: {Robert.Falkenberg, Karsten.Heimann, Christian.Wietfeld}@tu-dortmund.de

Remark:

These case studies can't cover many possibilities exposed.

Depend on the problems of your interest

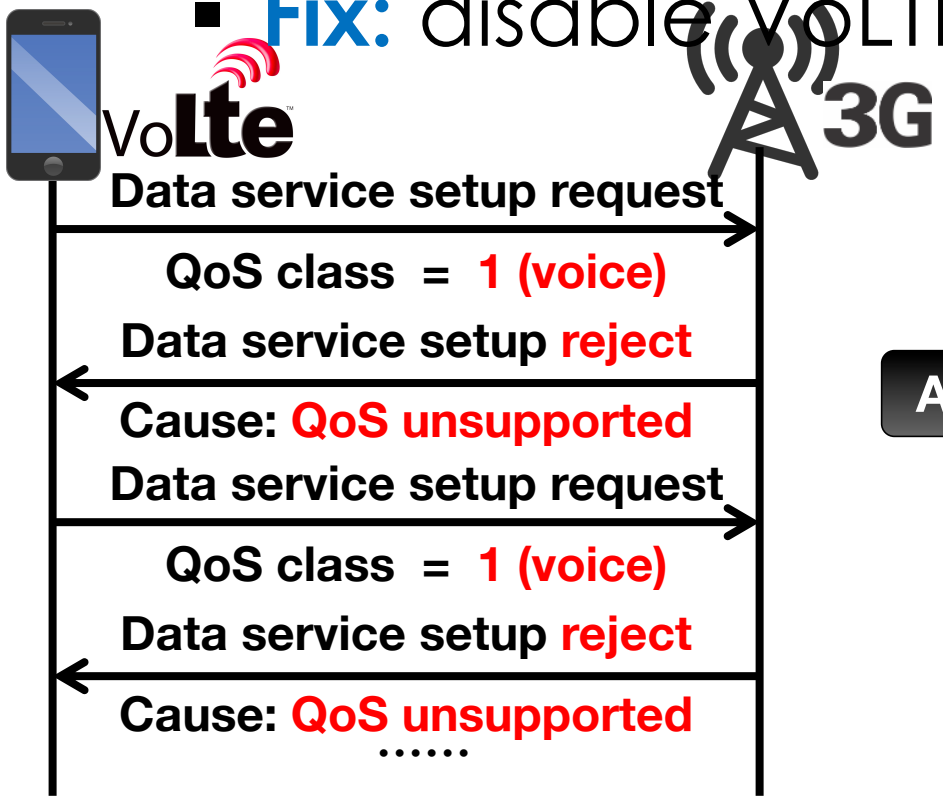
A Simple Case Study

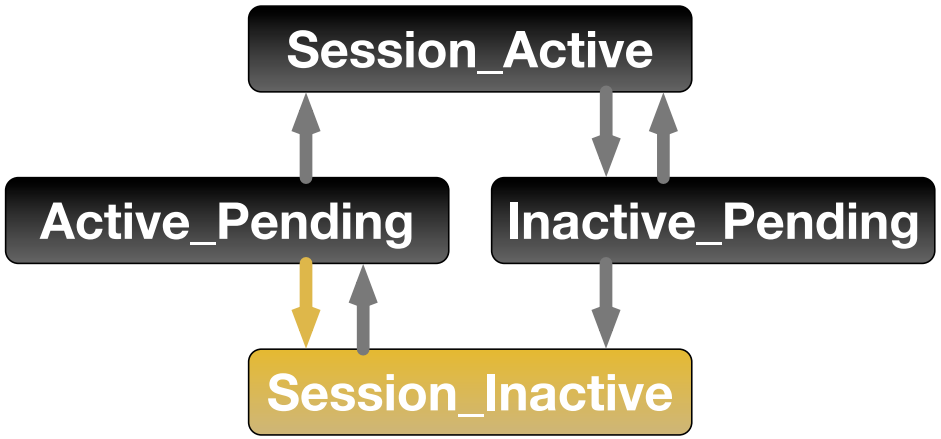


Good radio quality,
Why no data?

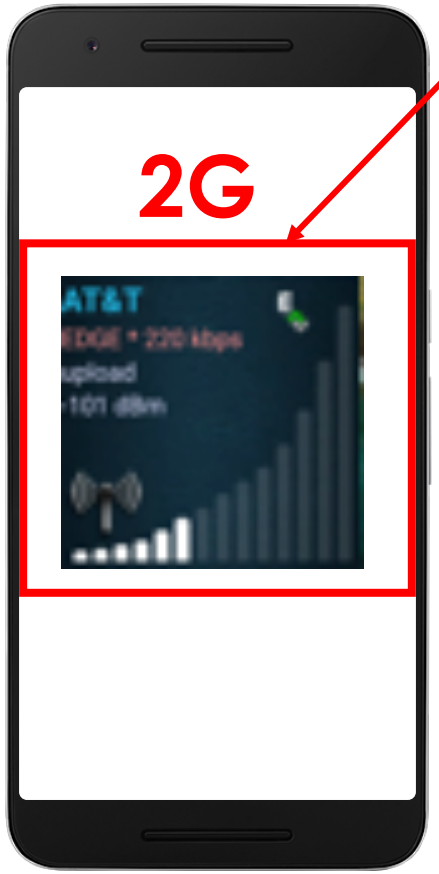
With MobileInsight,

- Analyze cellular messages exchanged
  - Track protocol state dynamics
- **Cause:** device-side misconfiguration
  - **Fix:** disable VoLTE when the device in 3G





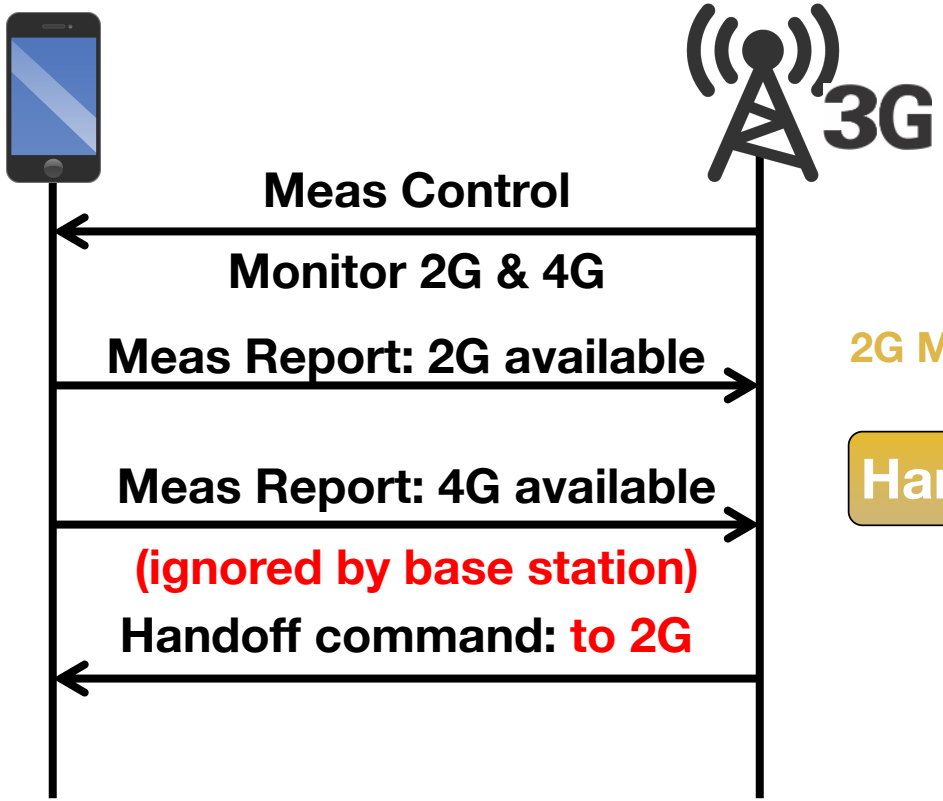
Another Case Study

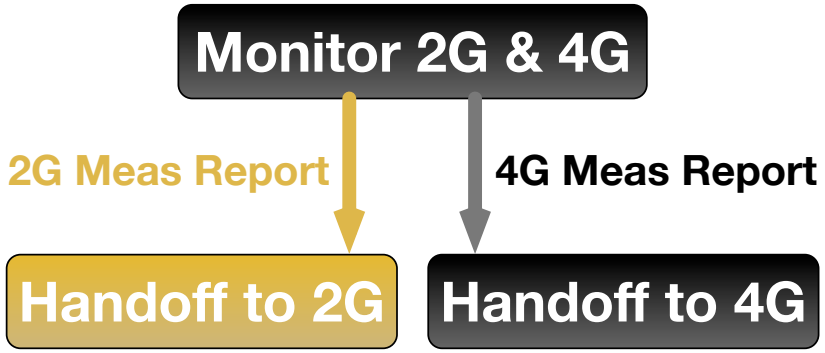


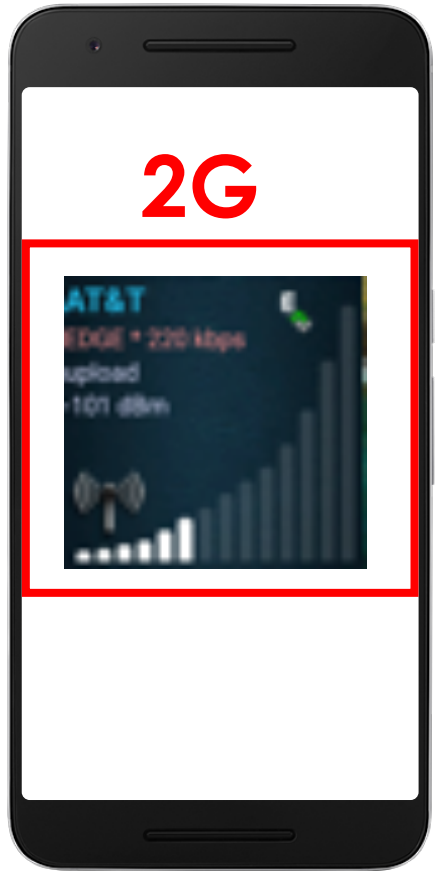
Why 2G, not 4G when 4G available?

With MobileInsight,

- **How:** Analyze inferred handoff decision logic



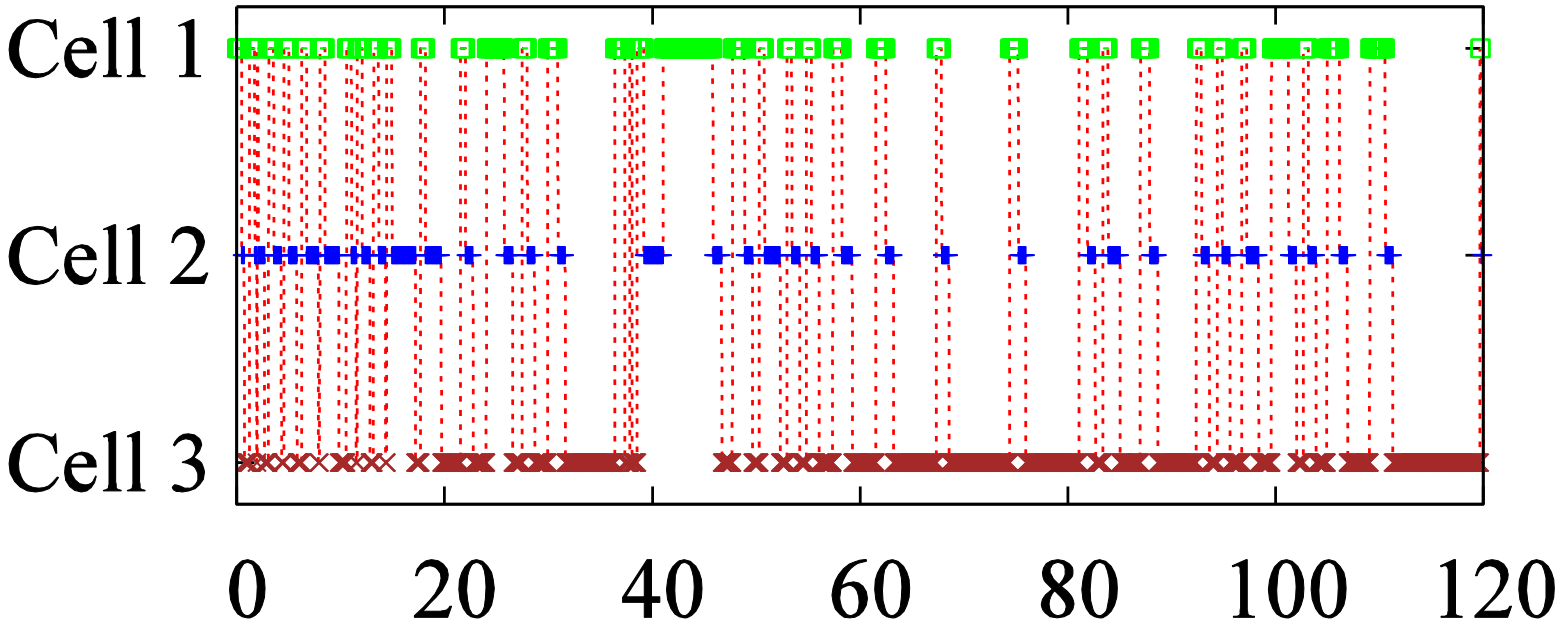




Next, A Formal Method

- To verify mobility management
  - Mobility: a salient feature
  - Via handoff (switching the serving cell)

Real-world Observation

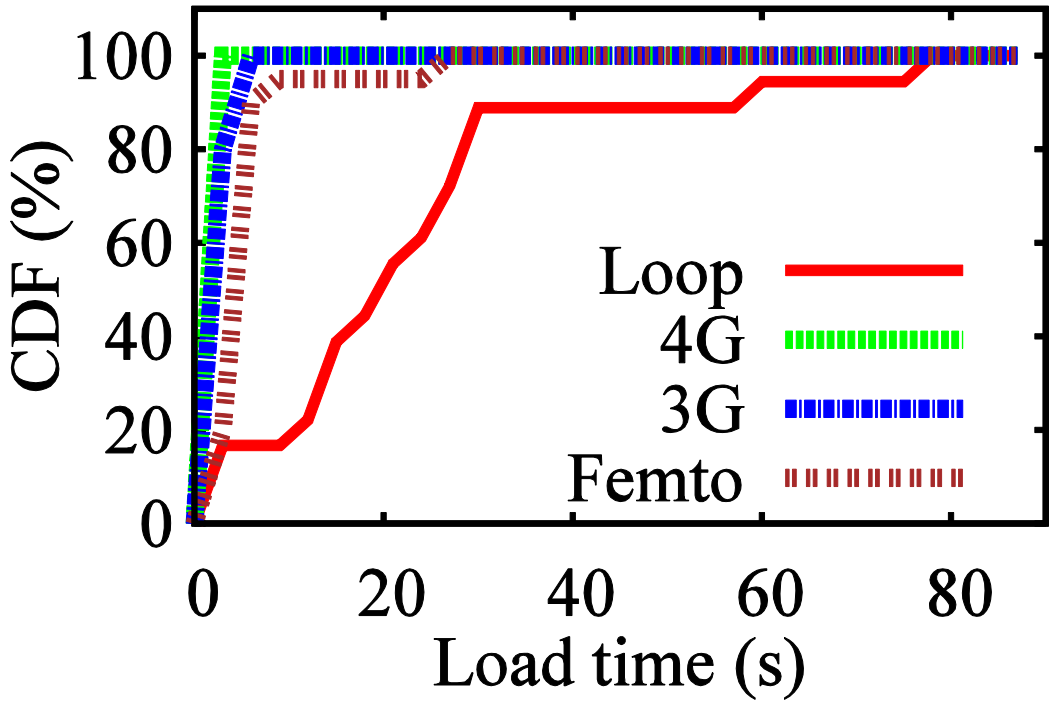


- Persistent loop under static conditions
  - @fixed location, constant radio quality
  - No convergence to any base station

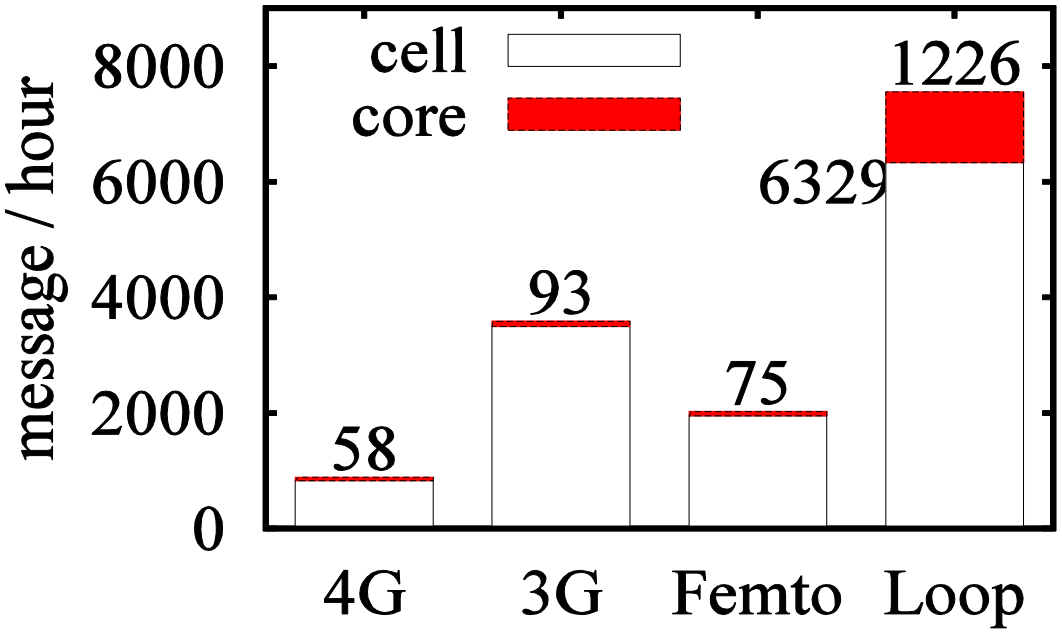
Negative Real-World Impacts

- Harm the device and network

Webpage performance degrade

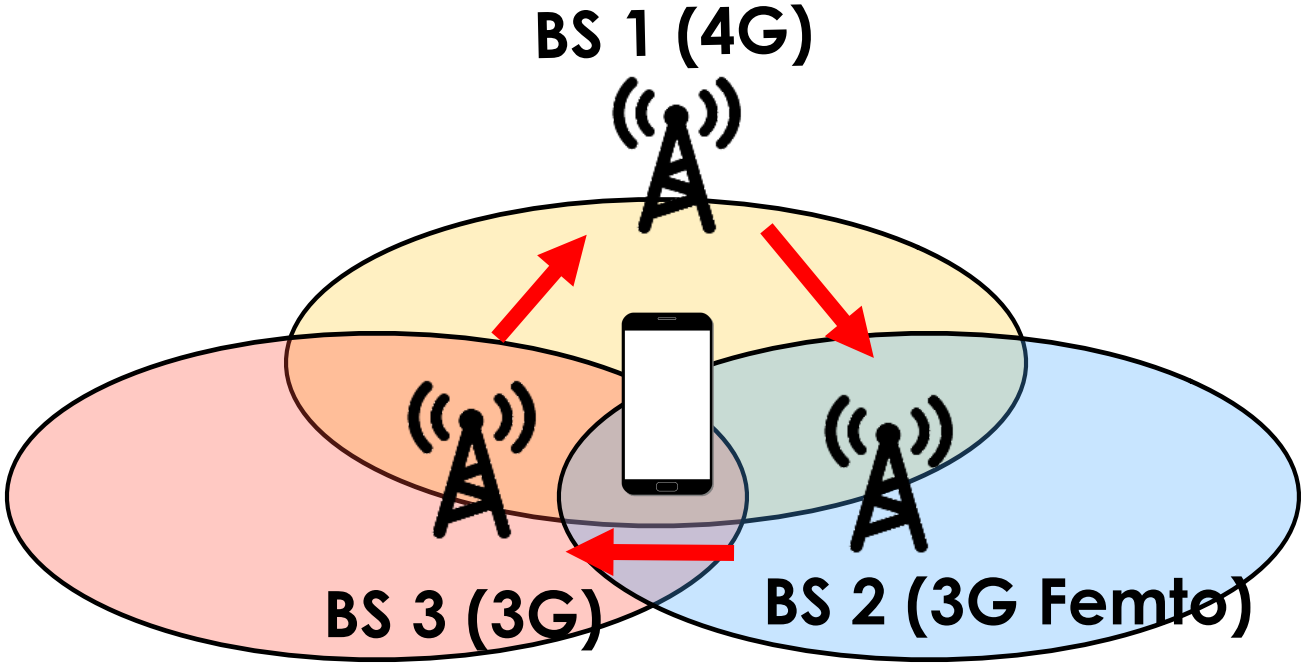


Signaling overhead



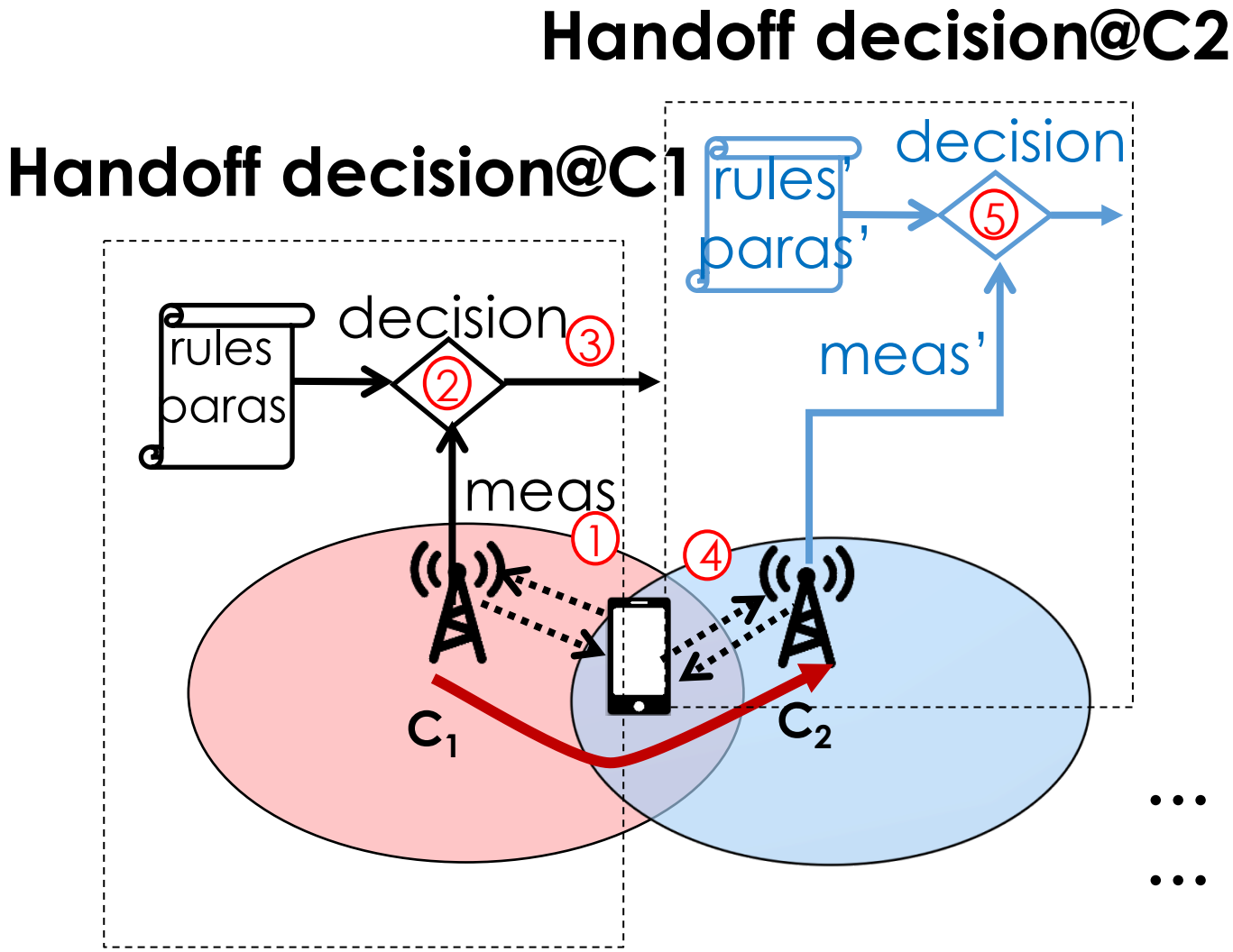
	Web load (s)	Signaling (msg/hr)
w/o loop	3	58
w/ Loop	76 **(25x)**	1226 **(23.5x)**

How Can This Loop Happen?



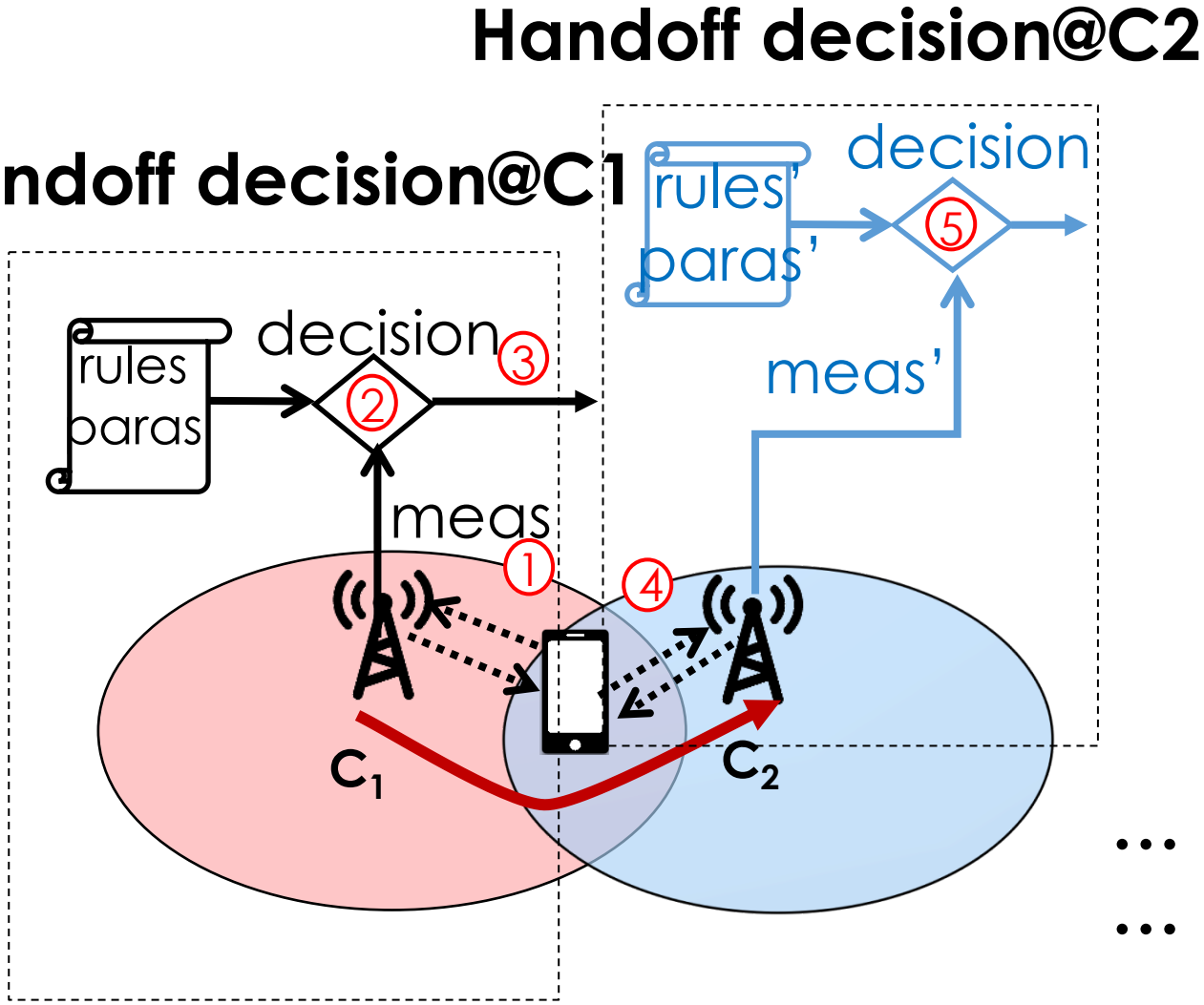
How a Handoff is Performed?

- Handoff: switch the serving cell
  - Likely based on radio strength
  - E.g., Idle-state handoff (cell-reselection)
  - Regulated by 3GPP standards



How a Handoff is Performed?

- Management-plane
  - Decision logic
  - Parameter configurations
  - E.g., radio quality thresholds, preferences, …
- **Distributed**
  - Local parameters & logic
- **Diverse**
  - For versatile demands

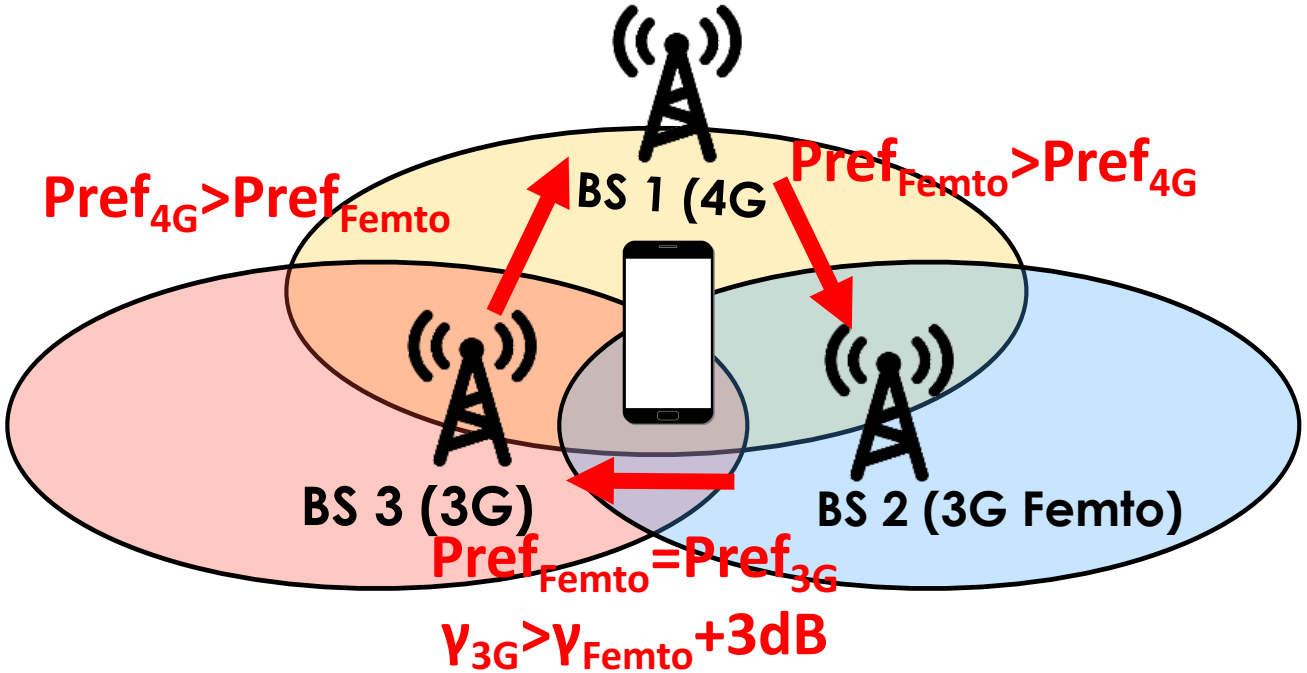


This Example: Policy Conflicts

- Configurable, local policies
  - BS 1 (4G): $Pref_{Femto} > Pref_{4G} > Pref_{3G}$
  - BS 2 (Femtocell): $Pref_{Femto} = Pref_{3G}$, no config to 4G
  - BS 3 (3G Macrocell): $Pref_{4G} > Pref_{3G} = Pref_{Femto}$

Well-justified local policy
≠ Global correctness

The preference settings are not consistent!



From Example to Generalization

Handoff instability

- What is handoff instability?
- Will it occur in real networks?
- Why will it occur?
- How to resolve it?

From Example to Generalization

Formulation: Discrete Event System

- Each handoff decision event: $s \rightarrow [t = H_s(C,P)]$
  - s, t: Serving/target base station
  - H_s: Decision logic in s
  - C: candidate base stations
  - P: Configurable parameters
- Handoff sequences:

$$s \rightarrow c_1 \rightarrow \ldots \rightarrow c_i \rightarrow [c_{i+1} = H_{ci}(c_i)] \rightarrow \ldots \rightarrow t$$

Stability: for any ***static*** conditions, any handoff sequence eventually converges to a single cell t

Theoretical Results

- Handoff instability does exist!
  - Not loop-free
  - Depends on handoff configurations
  - Similar to a well-known problem of BGP instability

Theoretical Results

Necessary/sufficient conditions

Stability: depends on policy logic & configurations

Theorem-1 (Preference-Threshold Conflicts)

Given n base stations $c_1, c_2, \ldots, c_n$, the convergence is guaranteed, **if and only if** for **every two** base station c_i and c_j

- $\min_{c_i \to c_k} \Theta_{i,k}^{\text{high}} \geq \Theta_j^{\text{serv}}$ if $Pref_i > Pref_j$
- $min_{c_{j \to c_k}} \Theta_{j,k}^{\text{high}} \geq \Theta_i^{\text{serv}}$ if $Pref_i < Pref_j$
- $\Theta_{i,j}^{\text{eqn}} + \Theta_{j,i}^{\text{eqn}} \geq 0$ if $Pref_i = Pref_j$

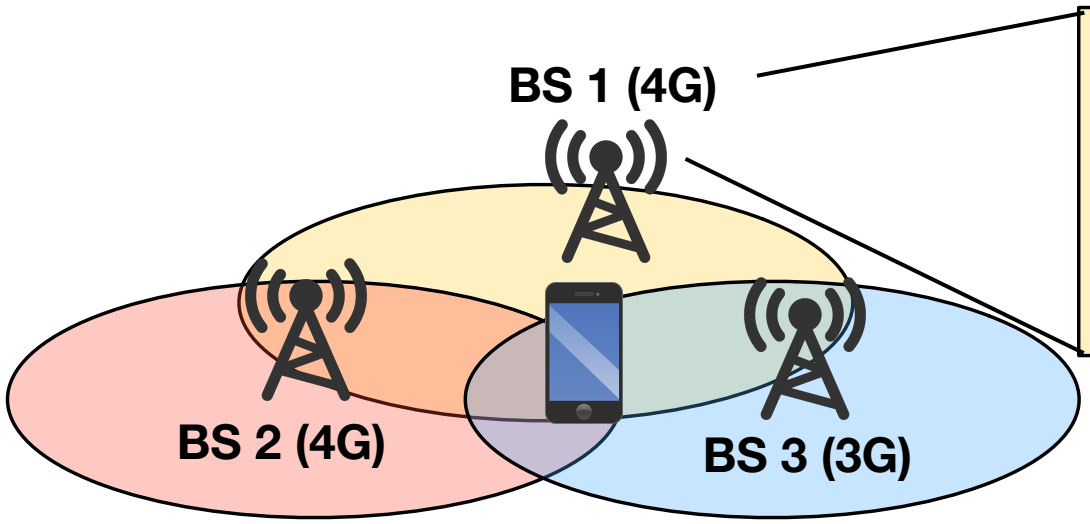
More conditions: preference-only conflicts, threshold-only conflicts, loop-prone decision logic, etc.

From Theory to Practice

- What are handoff configurations in the wild?
- What may be handoff misconfigurations?
- What are their real world impacts?

From Theory to Practice

- Operators: no such data released
- Our solution: Extracting and inferring handoff configurations through in-device MobileInsight

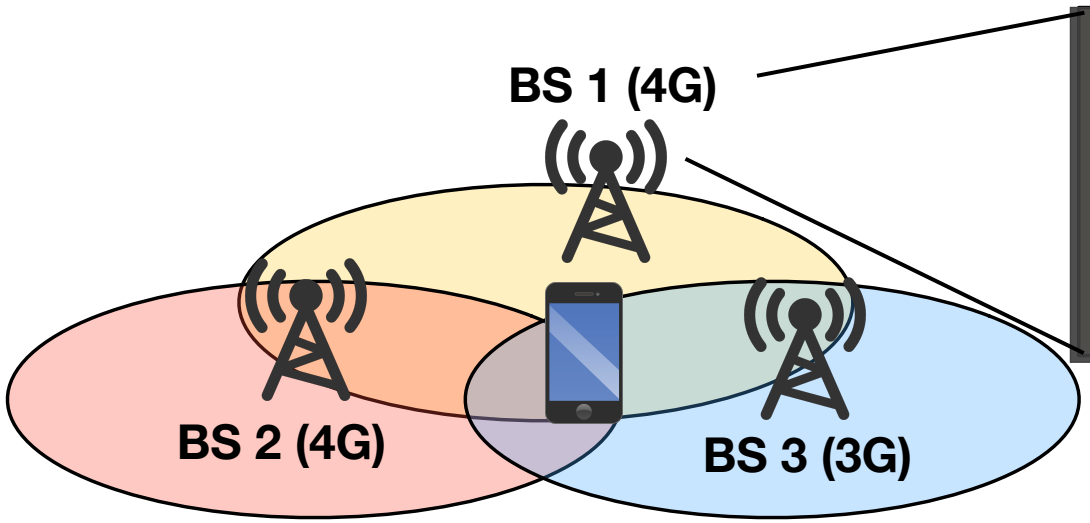


BS 1's handoff decision logic:

- Switch to BS 2 (4G) if $\mathrm{RSS}_{2(4G)} > \mathrm{RSS}_{1(4G)} + 3$ dBm
- Otherwise, switch to BS 3 (3G) if $\mathrm{RSS}_{1(4G)} < -110$ dBm and $\mathrm{RSS}_{3(3G)} > -90$ dBm

But, Inferring Handoff Logic is Hard

- **Challenge #1:** Non-standardized operations
- **Challenge #2:** Internal logic, not visible by end device



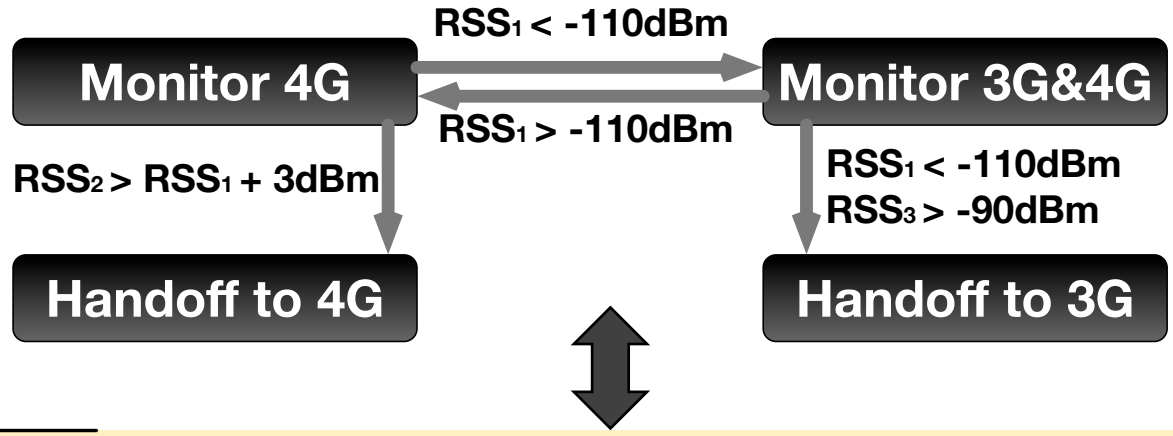
BS 1's handoff decision logic:

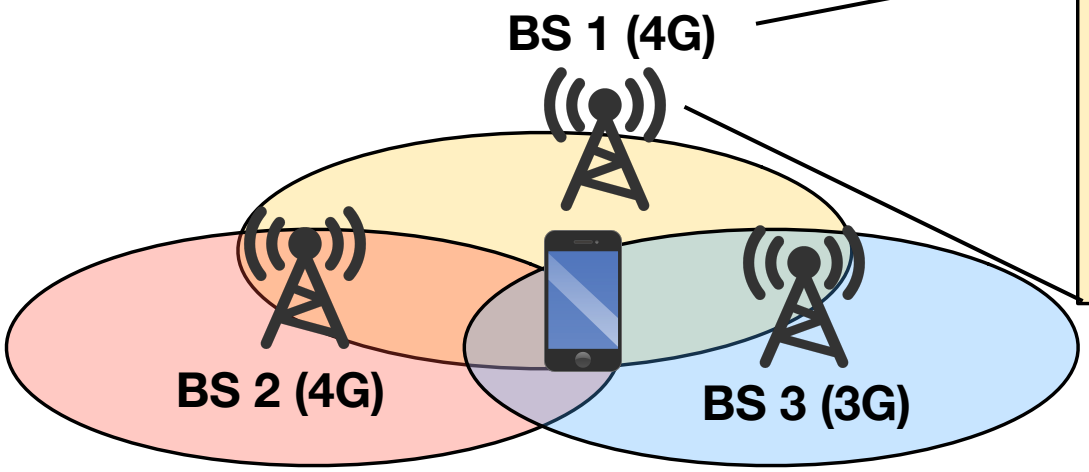
- Switch to BS 2 (4G) if $\mathrm{RSS}_{2(4G)} > \mathrm{RSS}_{1(4G)} + 3$ dBm
- Otherwise, switch to BS 3 (3G) if $\mathrm{RSS}_{1(4G)} < -110$ dBm and $\mathrm{RSS}_{3(3G)} > -90$ dBm

?

How Does MobileInsight Learn it?

- **Opportunity #1**: Operation logics are **finitely stateful**





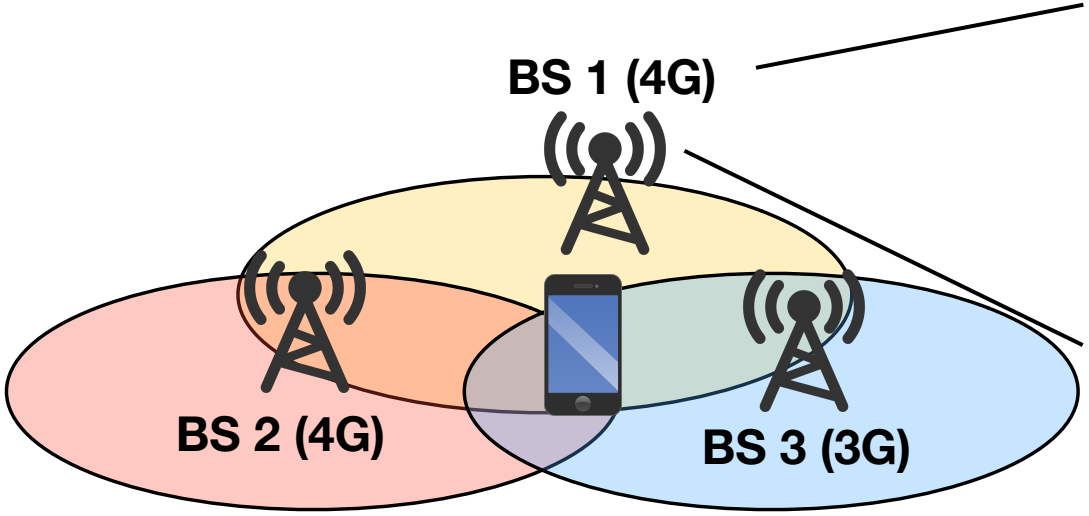
BS 1's handoff decision logic:

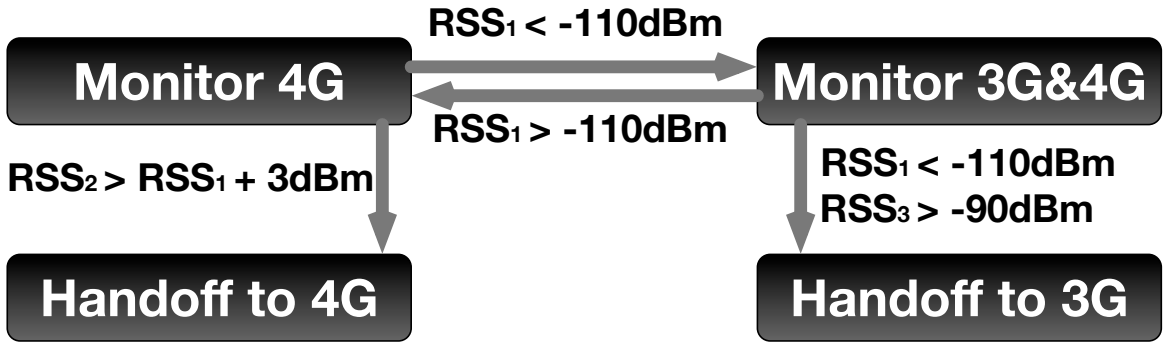
- Switch to BS 2 (4G) if $\mathrm{RSS}_{2(4G)} > \mathrm{RSS}_{1(4G)} + 3$ dBm
- Otherwise, switch to BS 3 (3G) if $\mathrm{RSS}_{1(4G)} < -110$ dBm and $\mathrm{RSS}_{3(3G)} > -90$ dBm

How Does MobileInsight Learn it?

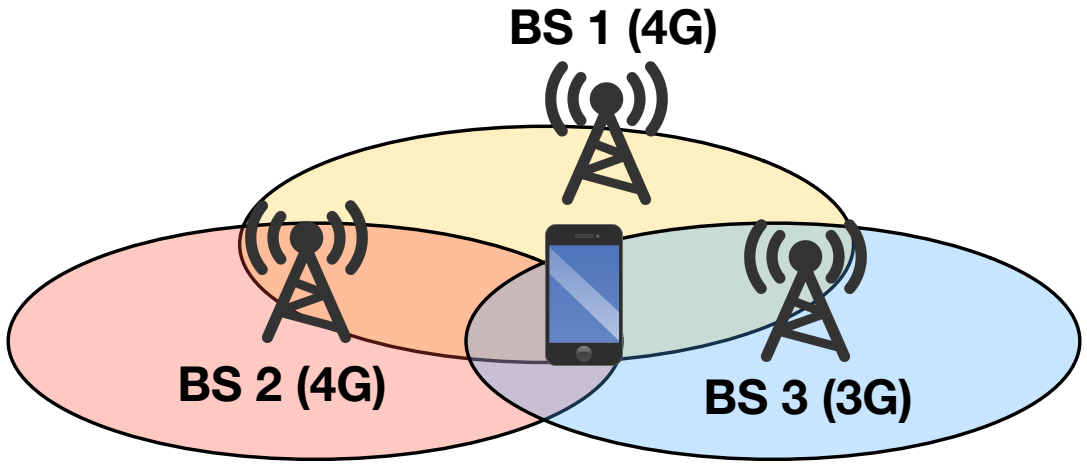
- **Opportunity #1:** Operation logics are **finitely stateful**
- **Opportunity #2:** Multiple observations

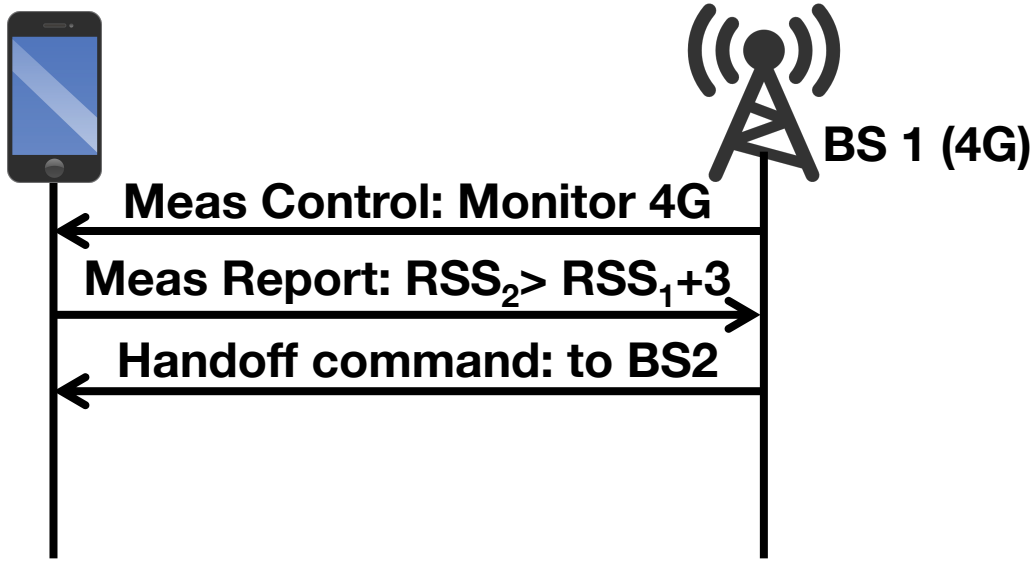
Solution: Online finite state machine learning

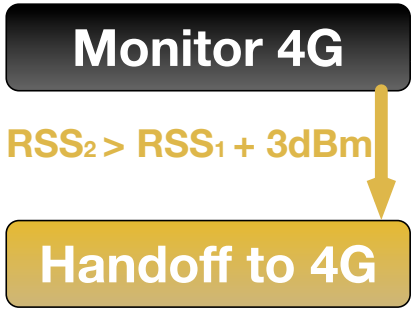




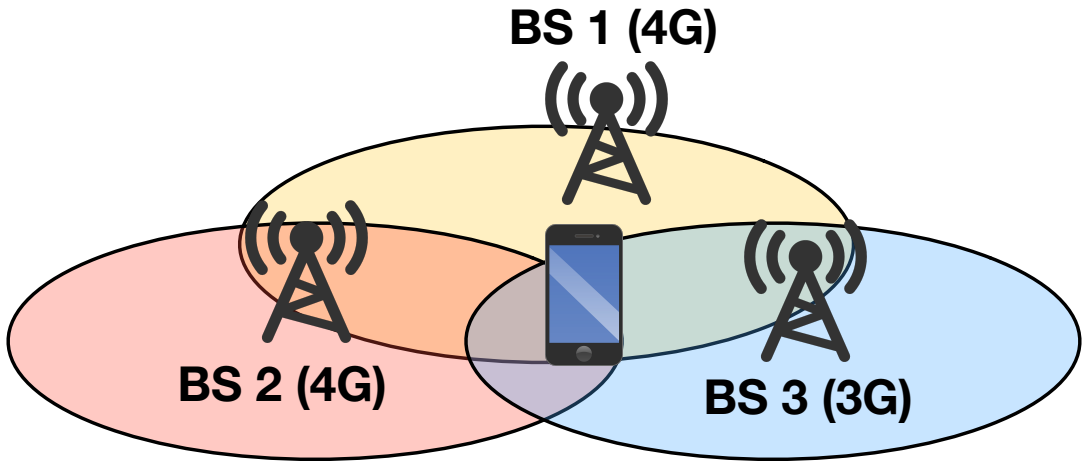
Online Finite State Machine Learning

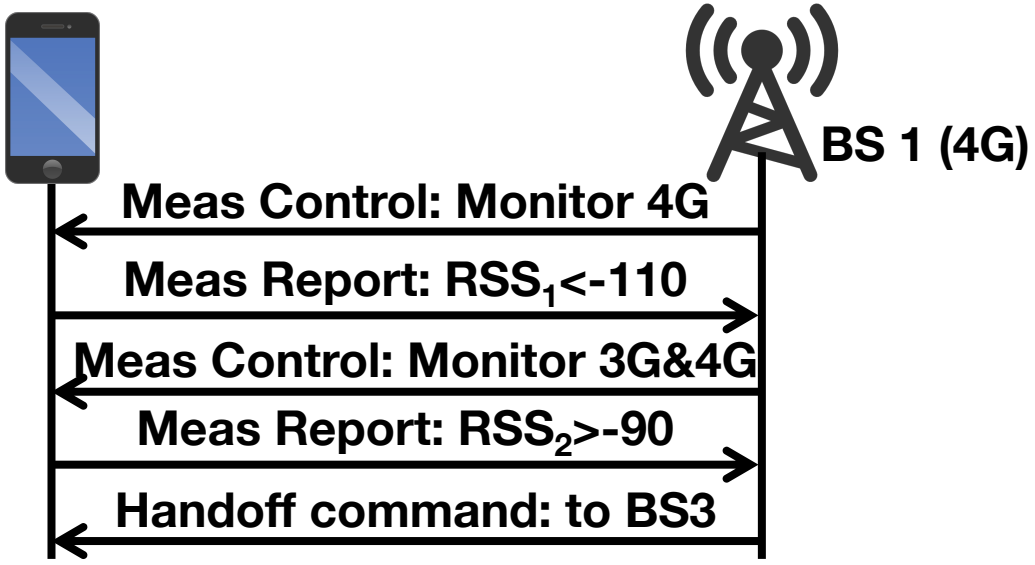


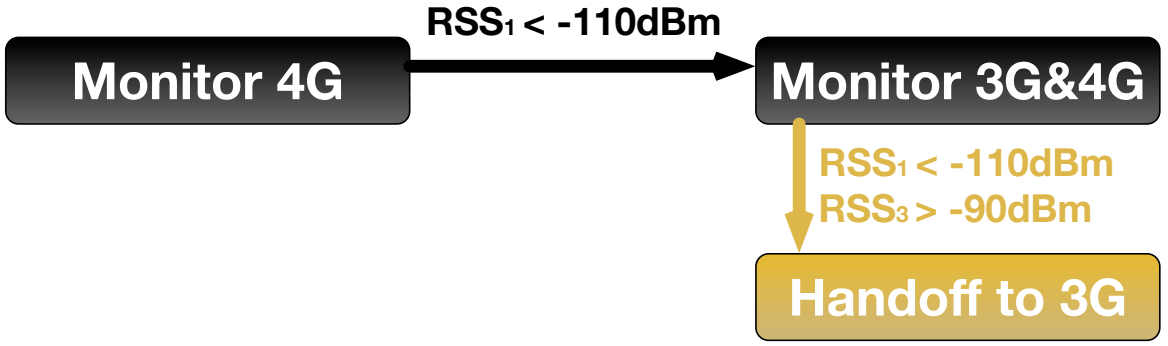




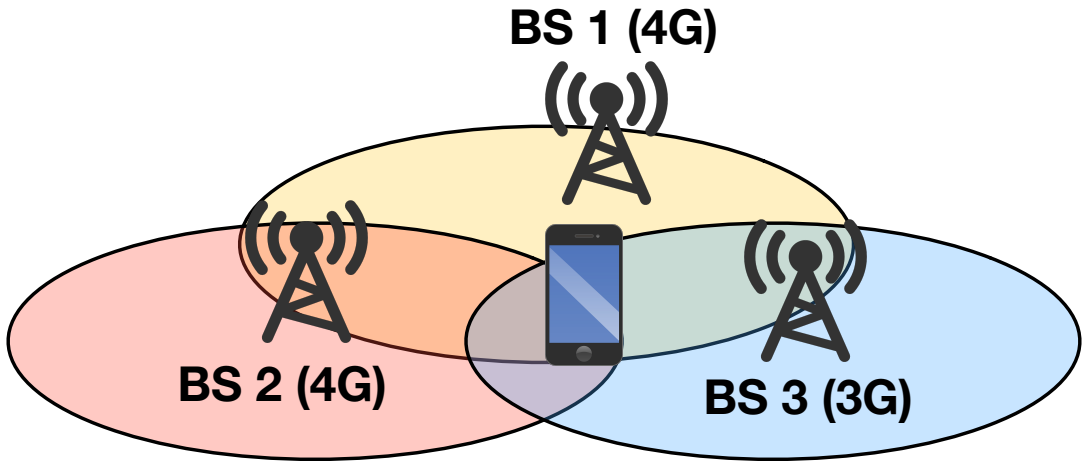
FSM Learning: Partial Recovery

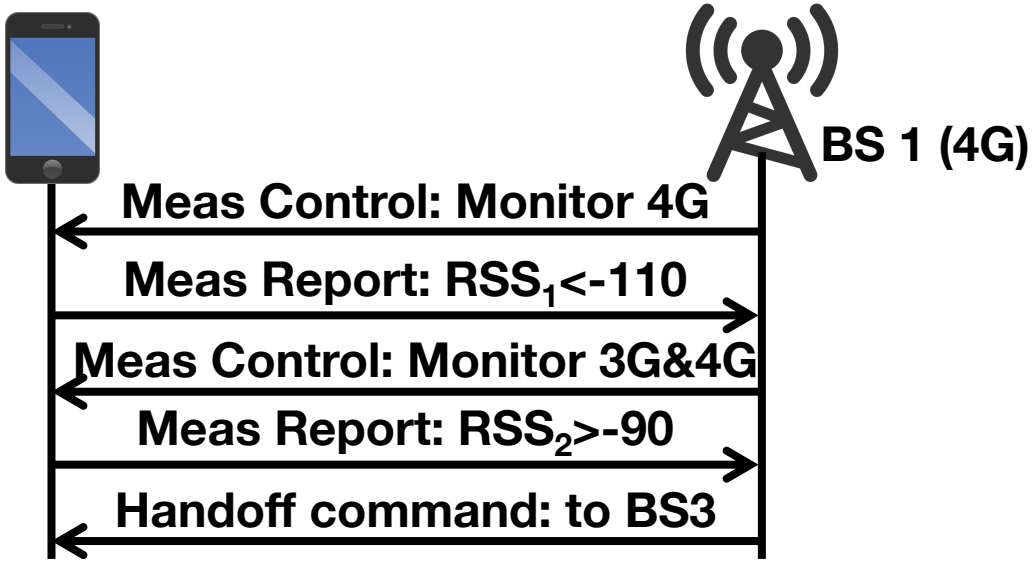


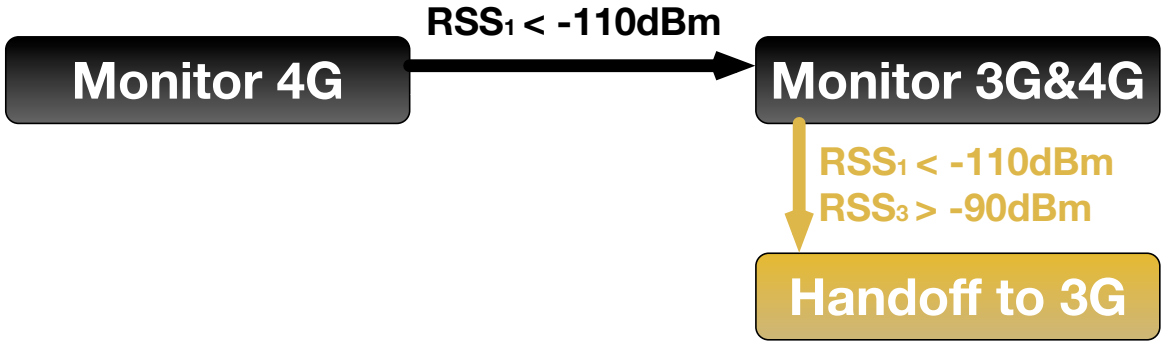




FSM Learning: Aggregation







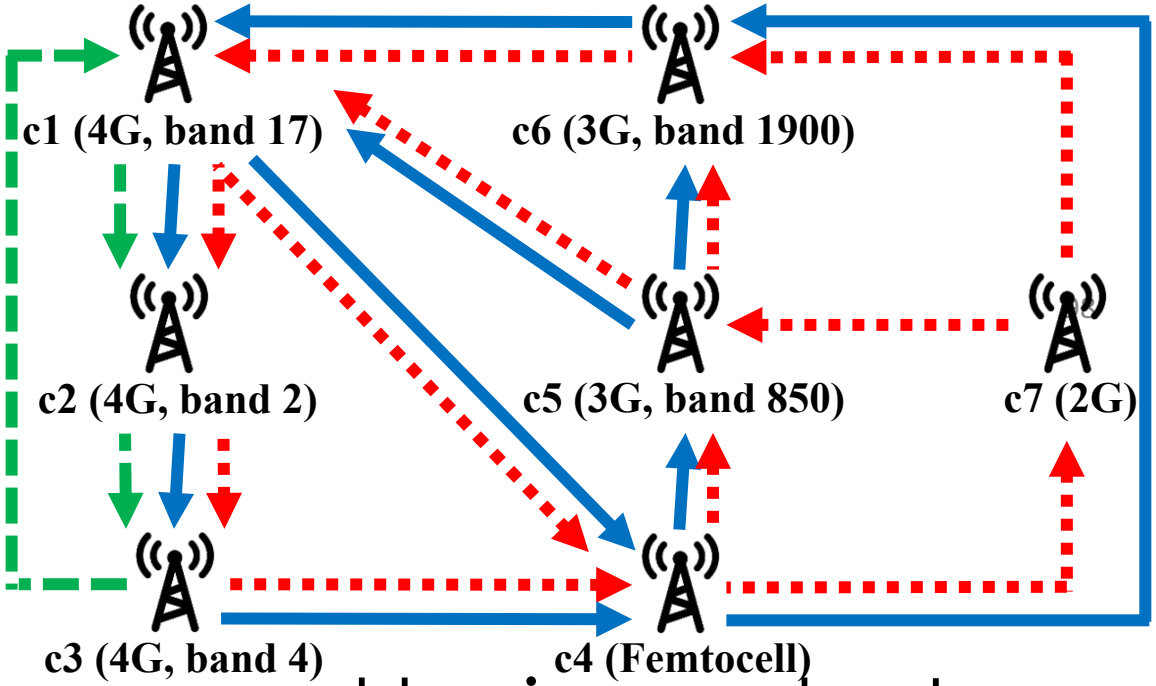
Inference Accuracy in Analytics

- **Inferring handoff logic:** 87.5%~95.3% accuracy
  - No ground truth → handoff prediction based on the handoff model we learnt
  - Via cross validation
  - **Note:** not all exposed by network (such accuracy implies invisibility)

	AT&T	T-Mobile	Sprint	Verizon
#Samples	11,050	10,178	10,042	2,741
Accuracy	90.7%	91.8%	95.3%	87.5%

Stability Violations in Real-World

- 21 classes of instances found in two U.S. carriers
  - Columbus, OH
  - Los Angeles, CA
  - 10/2015 – 02/2016



- Diverse causes
  - **4G-4G**: misconfiguration caused by imprudent infrastructure upgrade
  - **4G-Femto-3G**: policy conflicts
  - **4G-Femto-2G-3G**: device-side misconfiguration

Go Beyond

- Handoff unreachability [ICCCN'16]
  - E.g., handoff to 2G when 4G and 2G available
  - Another structural property
- A large-scale study (ongoing, join us)
  - At other places (countries)
  - Different carriers
  - In-depth analysis for handoff misconfigurations
- Insight to 5G
  - HetNets: small cells, mmWave cells, cellular & non-cellular

Many Other Opportunities

Examples: 3 papers at MobiCom'17

- Experience: An Open Platform for Experimentation with Commercial Mobile Broadband Networks

- Adding the Next Nine: An Investigation of Mobile Broadband Networks Availability

- Experience: Automating Diagnosis of Cellular Radio Access Network Problems

Many Other Opportunities

Examples: 3 papers at MobiCom'17

- Experience: An Open Platform for Experimentation with Commercial Mobile Broadband Networks
  - You couldn't do it because they used the platform deployed by Simula Research Laboratory
  - But you can do it if you or we deploy multiple phones in different carriers (crowdsourced MobileInsight)
- Adding the Next Nine: An Investigation of Mobile Broadband Networks Availability
- Experience: Automating Diagnosis of Cellular Radio Access Network Problems

Many Other Opportunities

Examples: 3 papers at MobiCom'17

- ❑ Experience: An Open Platform for Experimentation with Commercial Mobile Broadband Networks
- ❑ Adding the Next Nine: An Investigation of Mobile Broadband Networks Availability
  - You couldn't do it because you had no data from the platform deployed by Simula Research Laboratory
  - You can do it once you or we deploy crowdsourced MobileInsight
- ❑ Experience: Automating Diagnosis of Cellular Radio Access Network Problems

Many Other Opportunities

Examples: 3 papers at MobiCom'17

- ❑ Experience: An Open Platform for Experimentation with Commercial Mobile Broadband Networks
- ❑ Adding the Next Nine: An Investigation of Mobile Broadband Networks Availability
- ❑ Experience: Automating Diagnosis of Cellular Radio Access Network Problems
  - You couldn't do it because they used data from operators
  - You can do it if you or we use MobileInsight to collect bearer-level info

Open Research Opportunities

Unveil & understand real problems

Sample projects:

- ✓ Network diagnosis
- ✓ Network verification
- • Mobile big data analytics
- • …

Improve performance , efficiency, reliability

Sample projects:

- • **Cross-layer optimization**
- • Security enhancement
- • Protocol optimization
- • …

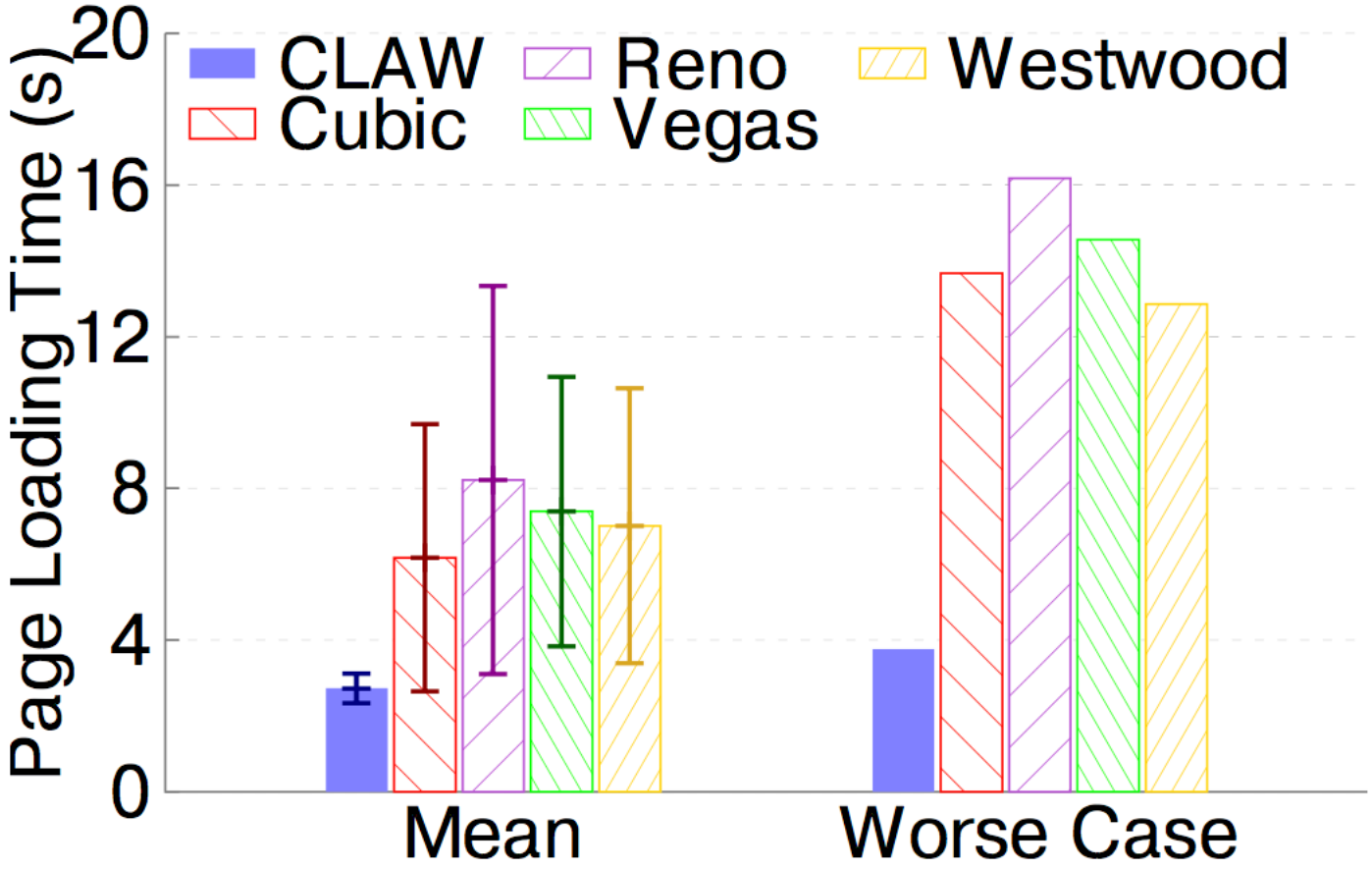
Mobile Web Loading Acceleration

- Xie et.al. (3rd-party) [Mobysys'17]
- Problem: Long delay (3 ~ 12+s over LTE)
- Cause: TCP doesn't adapt to real network conditions
  - TCP adaptation misled by large and unstable RTT
  - TCP overreacts to LTE link losses
  - Short web flows hinders the sending rate from quick convergence to the network bandwidth
- Core idea: using cellular link information to predict runtime bandwidth

Their Solution: CLAW

- CLAW (Cellular-Link-Aware Web-loading)
- TCP converges to net.bandwidth within one RTT
  - Estimate available resource
  - By harnessing LTE's PHY-layer statistics, including signal energy, packet loss and modulation scheme
  - Using what is available through the diagnostic interface (MobileInsight) at smartphones
- Details referred to their paper
  - RSRQ → cell load estimation → available resource for one client → real-time bandwidth estimation → combined with TCP adaptation → CLAW

CLAW Outperforms Existing TCP



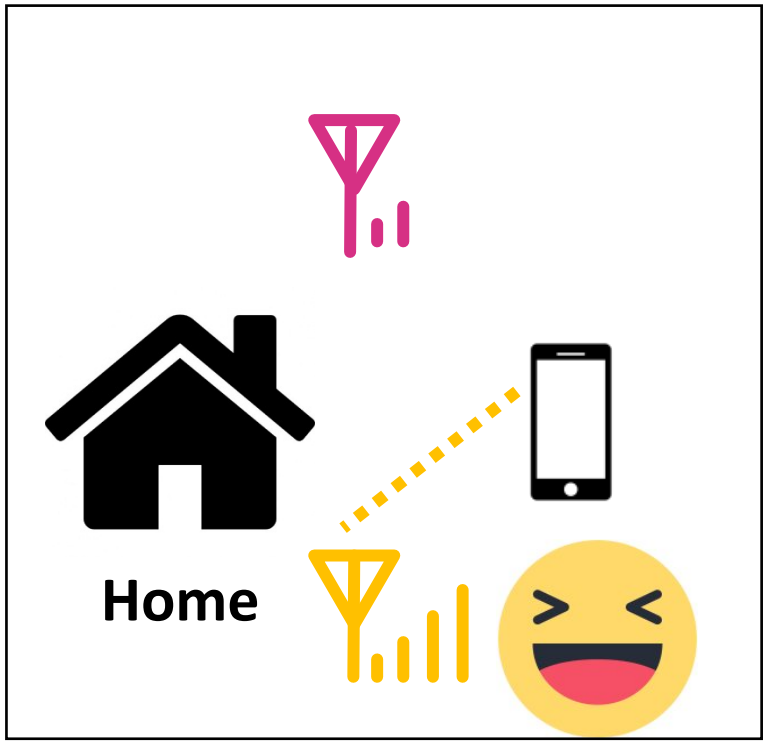
iCellular for Google Fi [NSDI'16]

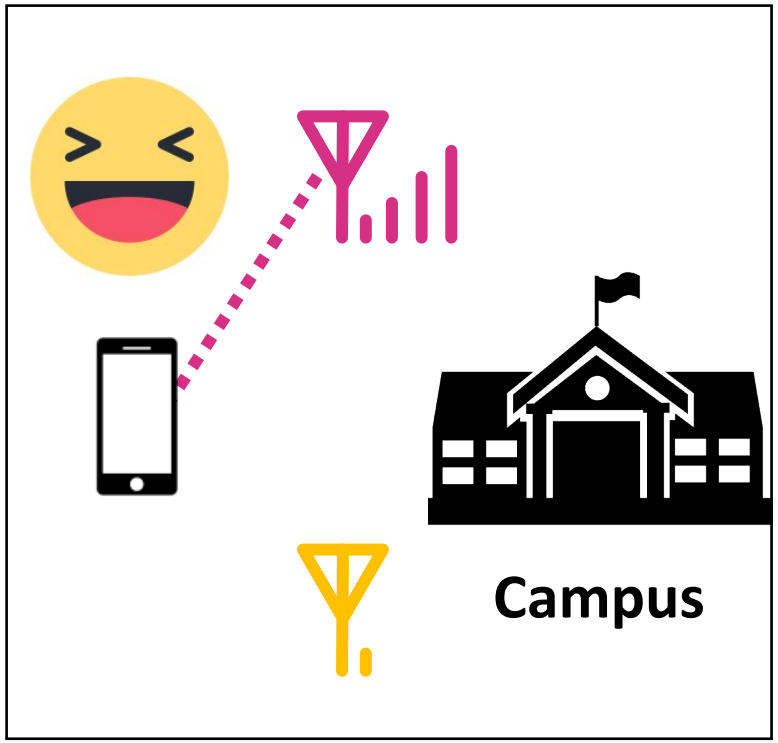
- boost wireless via multi-carrier access

Project Fi

T-Mobile

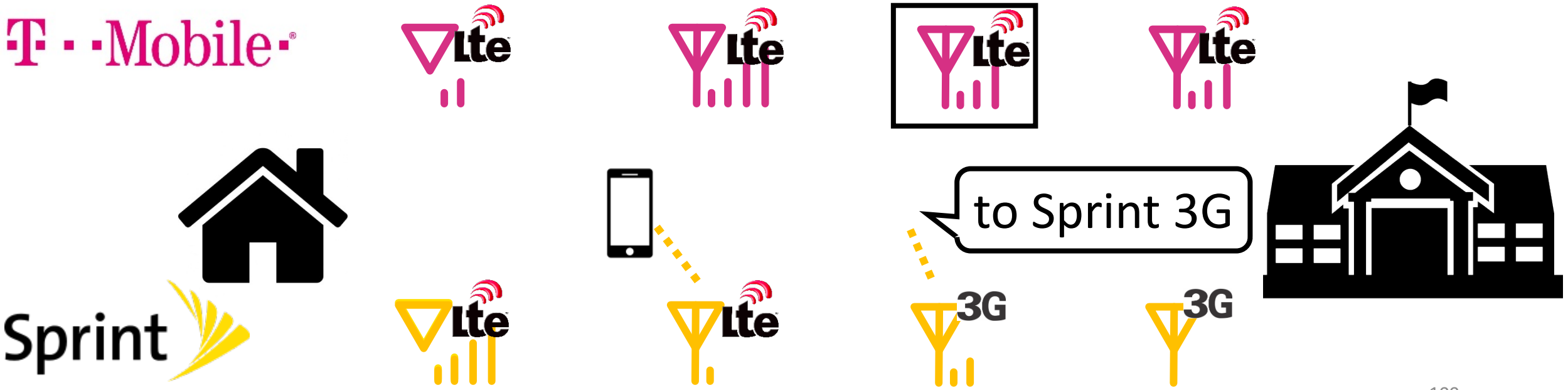
Sprint





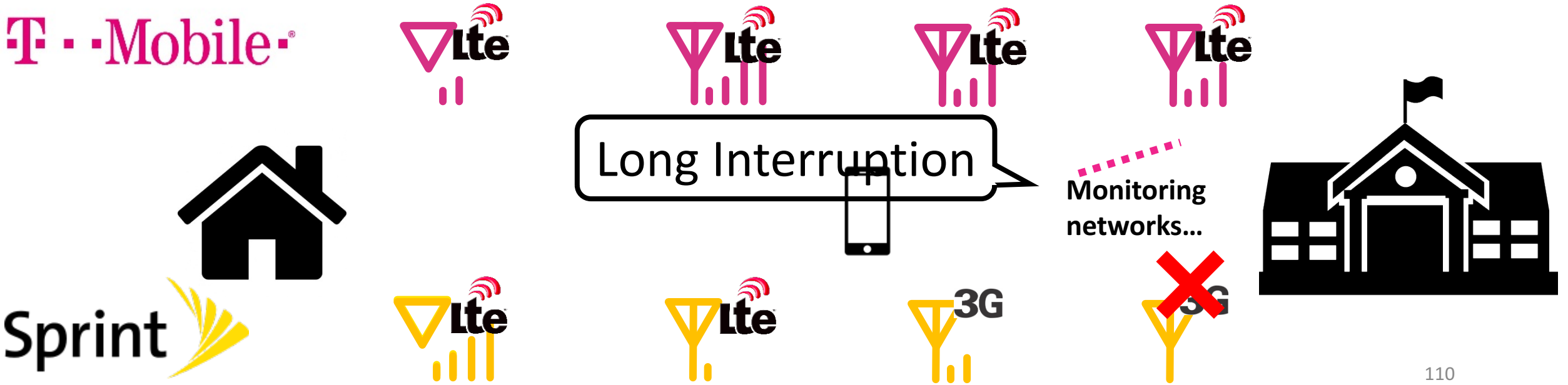
However, Two Downsides

- Make a worse choice



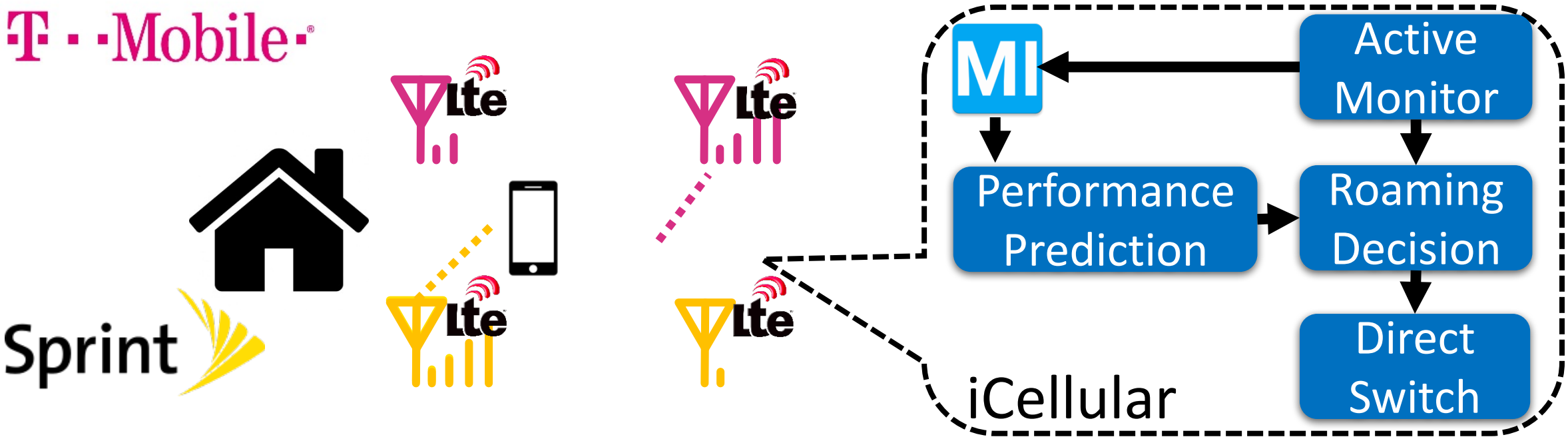
However, Two Downsides

- Make a worse choice
- Long disruption during the switch
- **Cause**: no cellular information @device
  - Passively follows whatever the networks asks it to do



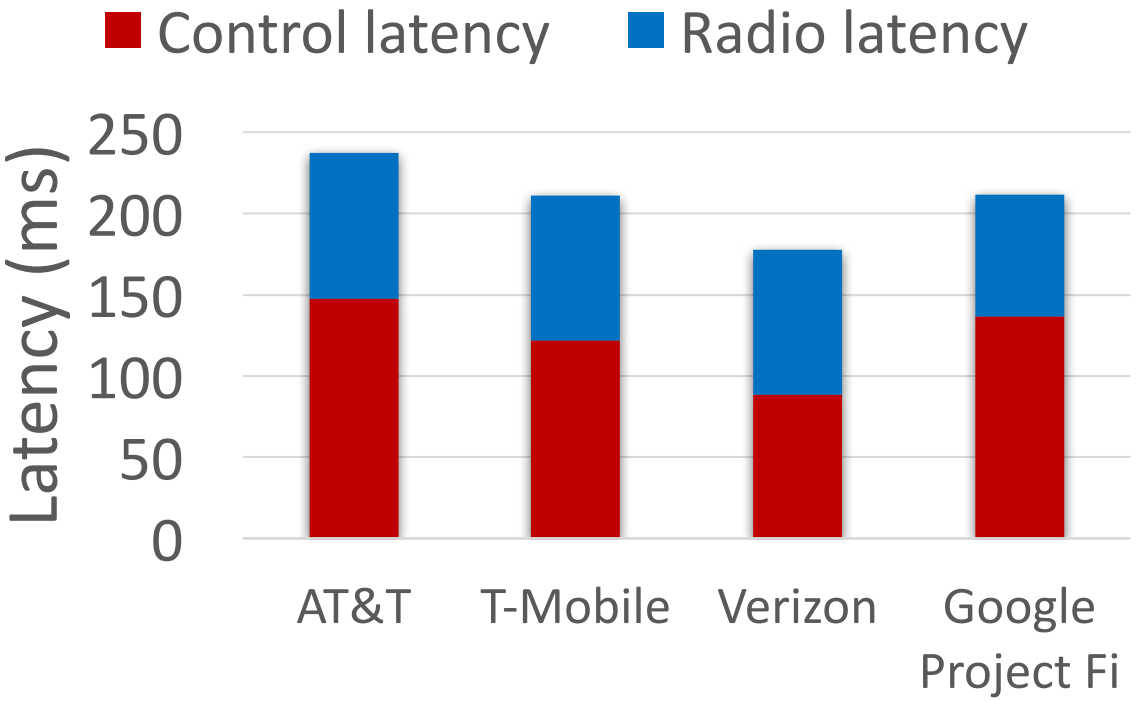
iCellular: A Client-side Solution

- **Proactive** selection with runtime net. info
  - Throughput: 23.8% on average, 3.74x at max
  - Latency: 60.4% on average, 1.9x at max

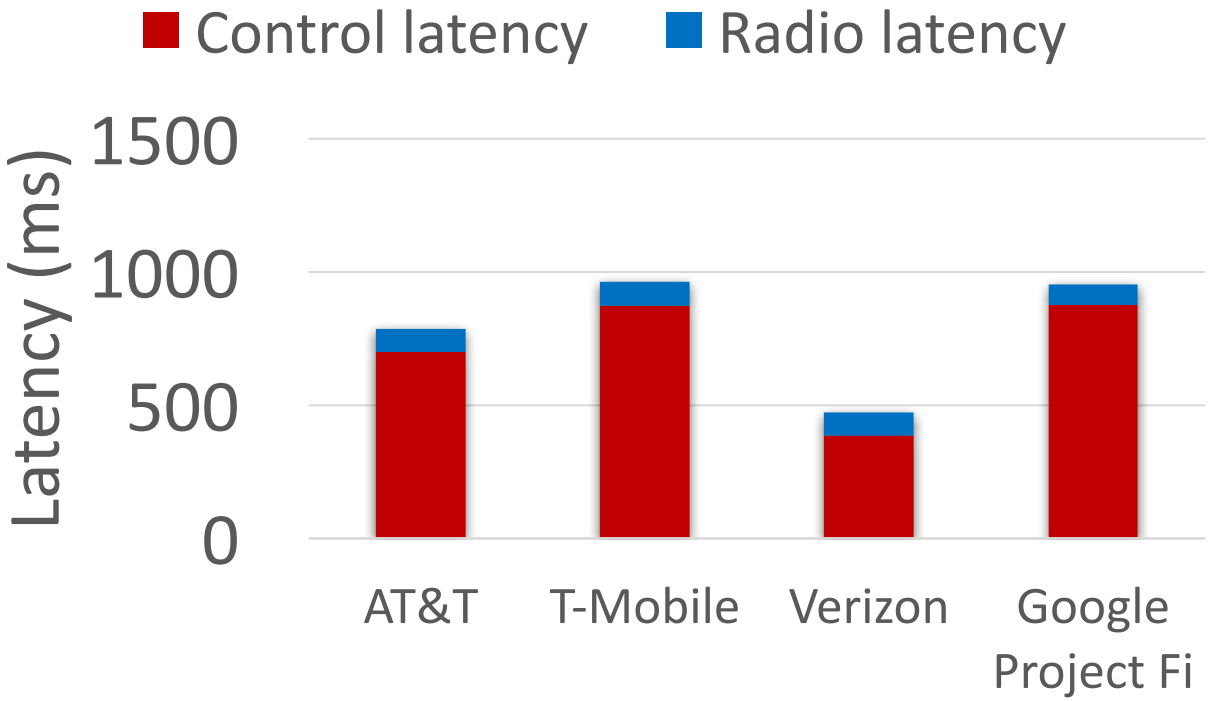


DPCM: Lower Latency in New Control-Plane Protocols [mobicom17]

- Problem: control-plane functions are slow that contribute to large latency



Static: data session establishment



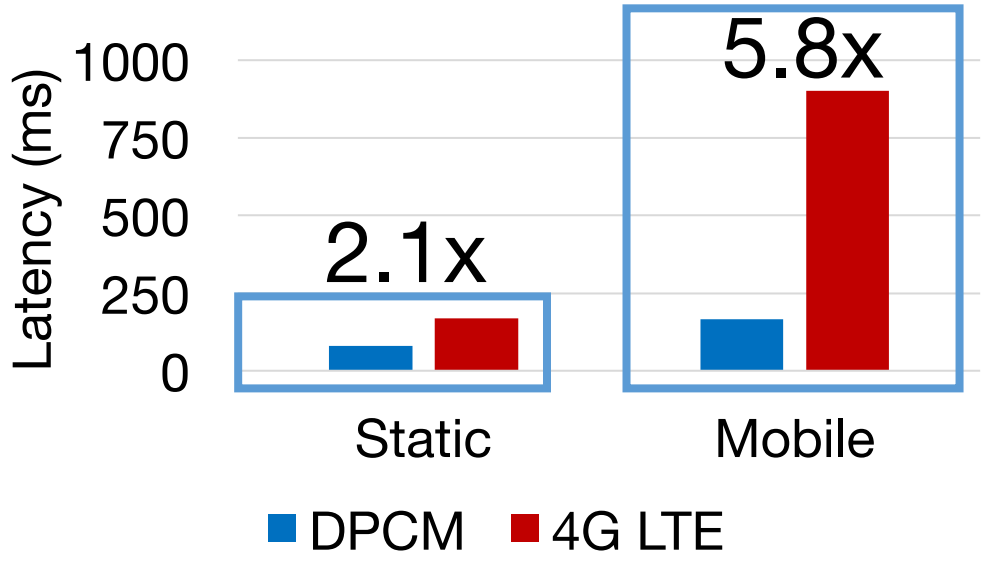
Mobility: location update

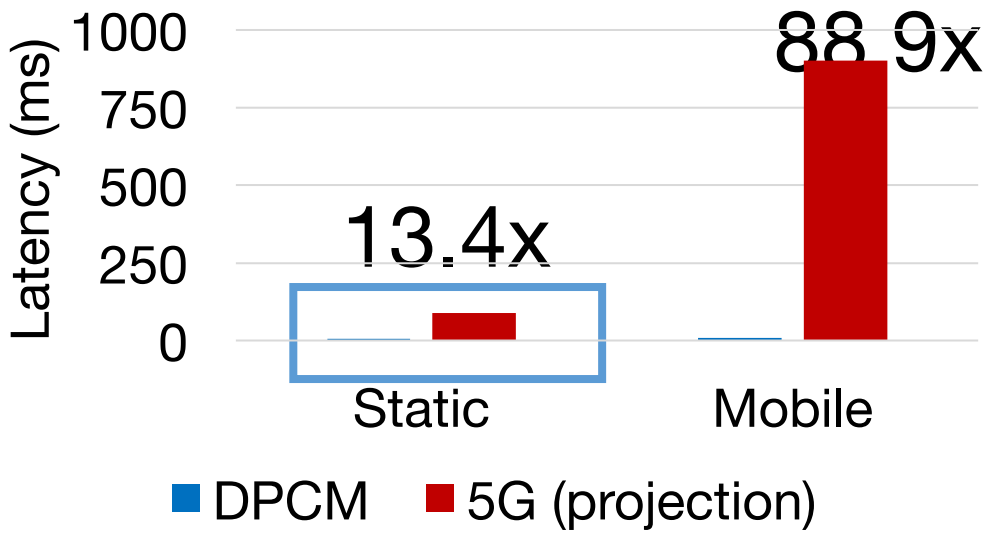
DPCM: From Cause to Solution

- **No data** until all control procedures are completed
- All the control plane procedures are **Sequential**
- Sequential procedures are **more than necessary**
- Accelerate it via **bypass, pipeline and parallelism**
  - Formulate its inherent dependence as state management

Latency Reduction via DPCM

- More latency reduction in mobility
- More reduction in failures (up to 11s, 11.5x)
- More critical (if 5G NR radio)
  - Control-plane latency dominates





5G New Radio Projection
(Assuming 1ms radio latency)

Still, Many Open Questions

- Low-latency support
  - Harness PHY-information to reduce extra delay caused by retransmission
  - Hints to TCP/application for cross-layer optimization
- Failure handling
  - Retrieve lower-layer hints for failures
  - Avoid or recover from failures quickly
  - Example: No network access due to rejection without a specific channel support
  - Solution: switch to a workable channel right away and avoid "no access" due to this failure

Demo #3: Extract Handoff Config.

- Optional

- Run MobileInsight (setting: control-plane)
- Manually switch RAT
  - Turn on flight mode and turn it off
  - Switch from LTE to 3G and even 2G
- Check the collected logs
  - Specific messages (e.g., LTE SIB3, SIB5, SIB6, SIB8)

This Tutorial: Agenda

- ✓ Introduction
- ✓ Tutorial overview
- ✓ MobileInsight: first look
- ✓ Primer on cellular protocols
- ✓ MobileInsight: second look
- ✓ Research opportunities and examples
- ⬇ **Advanced topics**

8. Closing remarks

Advanced Topics

- MobileInsight Usage
  - Offline Analyzer
  - Build your own analyzer
  - Develop your own plugin
- MiLAB: Open Experimentation Testbed

Offline Analyzer

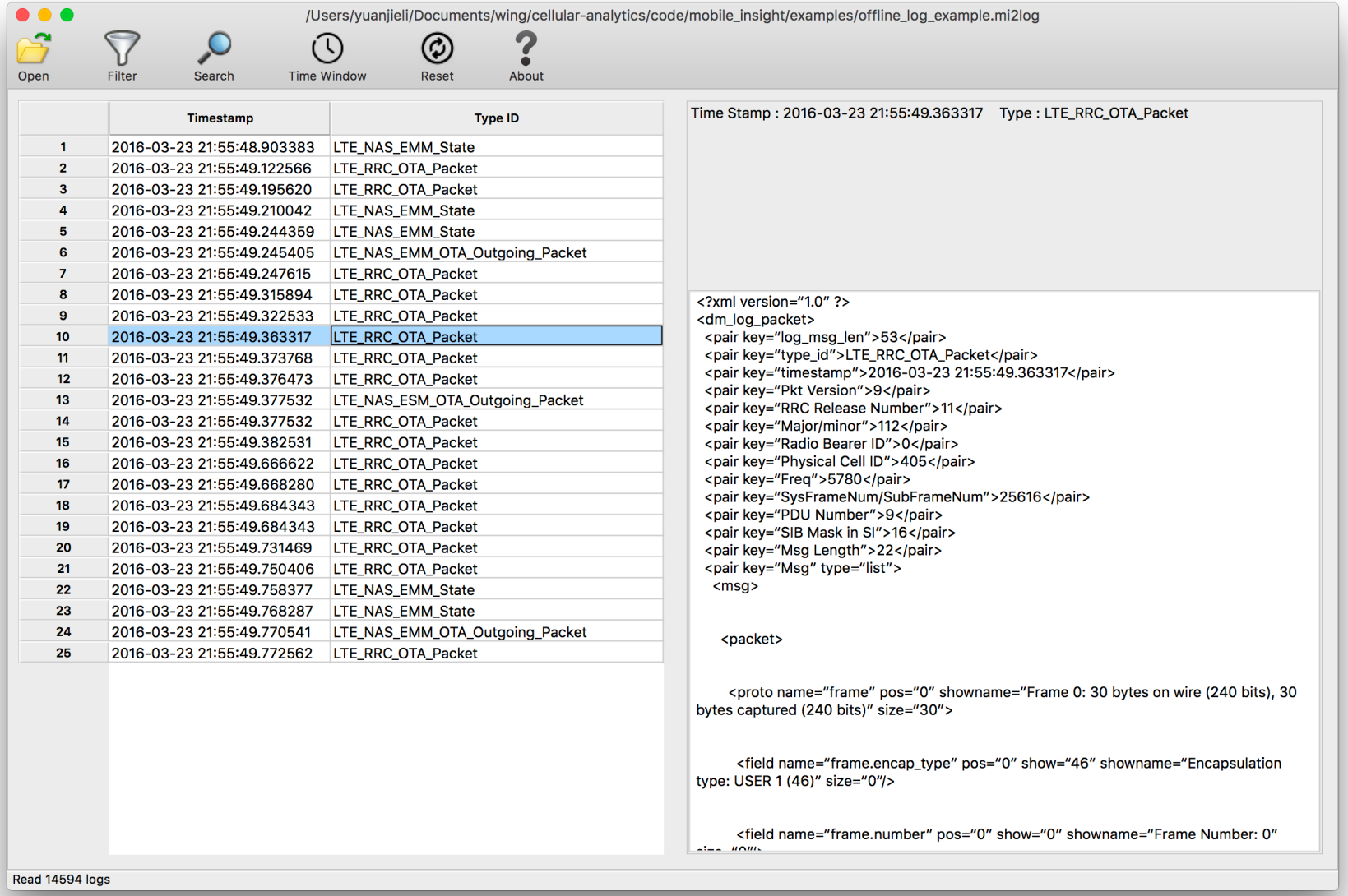
- For beginners (mobile users)
- Desktop analyzer of logs collected

- Step 1: Install MobileInsight-Core
  - ./install-macos.sh (macOS)
  - ./install-ubuntu.sh (Ubuntu)
- Step 2: Follow the example

- Git: https://github.com/mobile-insight/mobileinsight-core
- Tutorial: http://mobileinsight.net/get_started_desktop.html

GUI for Offline Analyzer

- GUI
  - > mi-gui
  - Files: *.mi2log



Offline Analyzer

- Follow our examples
  - lte-measurement-example.py
  - lte-nas-layer-example.py
  - monitor-example.py
  - msg-statistics-example.py
  - offline-analysis-example.py
  - offline-analysis-filtering.py
  - online-analysis-example.py

- Write your own analyzer

Develop Your Own Analyzer

- http://mobileinsight.net/desktop-part-ii-analyzer.html

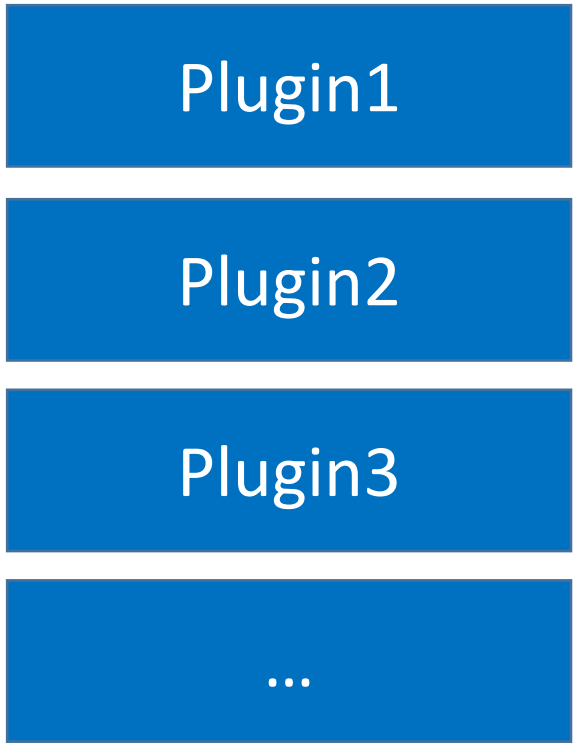
- Base class: Analyzer
- Declare its dependency on cellular message types: enable_log
- Declare analyzer dependency: include_analyzer
- Event-driven Callbacks

Default Analyzers

Analyze r	Descrip tion	Standar ds/Refere nce
lte_mac_analyzer .py	4G MAC protocol analyzer	TS36.321
lte_meas urement_ analyzer. py	Reports 4G-RRC measureme nt results	TS36.331
lte_nas_analyzer .py	4G EMM/ESM protocol analyzer	TS24.301
lte_pdcp _analyze r.py	4G PDCP protocol analyzer	TS36.323
lte_phy_analyzer .py	4G PHY layer (LL1) analyzer	TS36.213, TS36.211
lte_rlc_analyzer .py	4G RLC protocol analyzer	TS36.322
lte_rrc_analyzer .py	4G RRC protocol analyzer	TS36.331
umts_nas _analyze r.py	3G MM/GMM/SM /CM protocol analyzer	TS24.008
mobility_mngt.py	4G handoff decision logic inference	TS36.304, TS36.331, MobileIns ight paper [Mobicom’ 16]
wcdma_rr c_analyz er.py	3G-RRC protocol analyzer	TS25.331

Develop Your Own Plugin

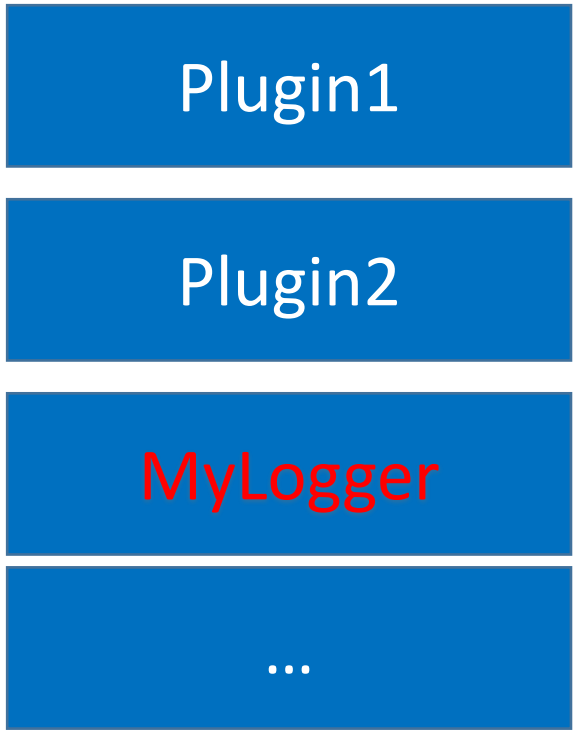
- Python-for-Android: Extensible
  - \sdcard\mobileinsight\plugins



Develop Your Own Plugin

- Example: add "MyLogger"

```
/sdcard/mobileinsight/plugins/
        Plugin1/
                main.mi2app
                readme.txt
                settings.json
        Plugin2/
                main.mi2app
                readme.txt
                settings.json
                __init__.py
                files/
        MyLogger/
                main.mi2app
                readme.txt
                settings.json
                 ...
        ...
```



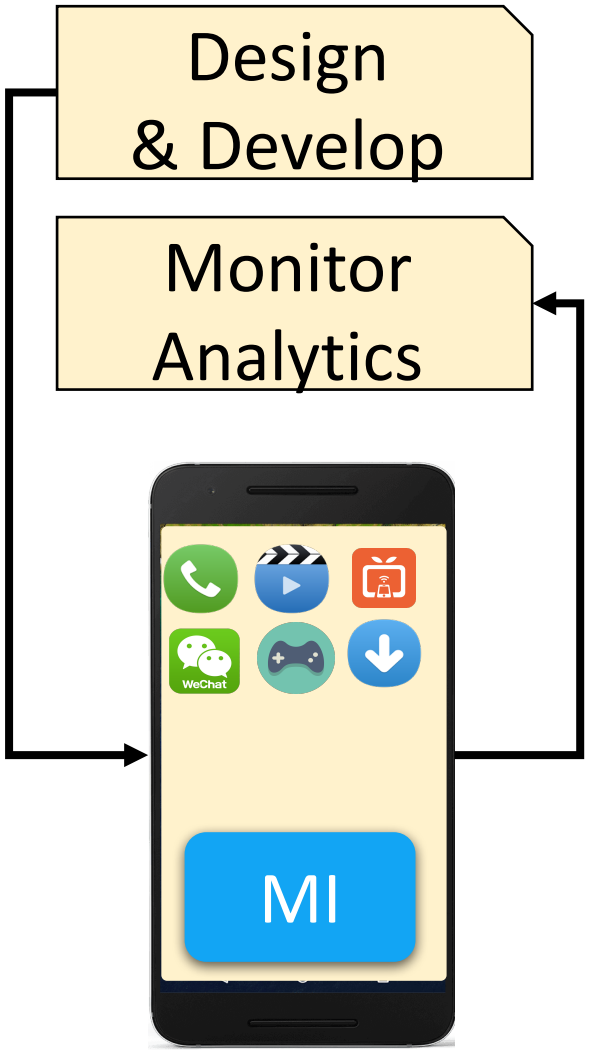
Advanced Topics

- MobileInsight Usage
  - Offline Analyzer
  - Build your own analyzer
  - Develop your own plugin

- MiLAB: Open Experimentation Testbed

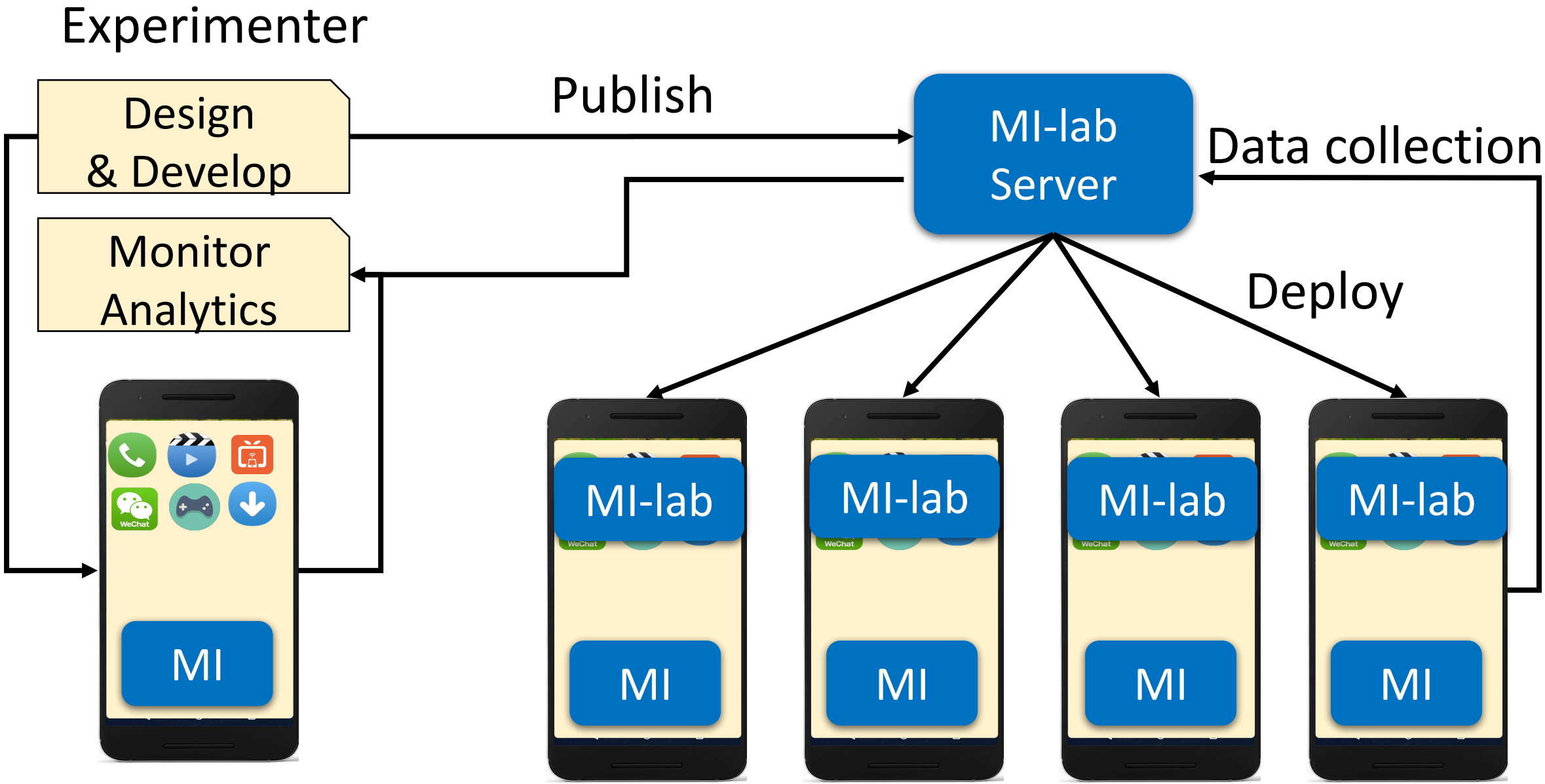
MiLAB: Open Experimentation Testbed

Experimenter



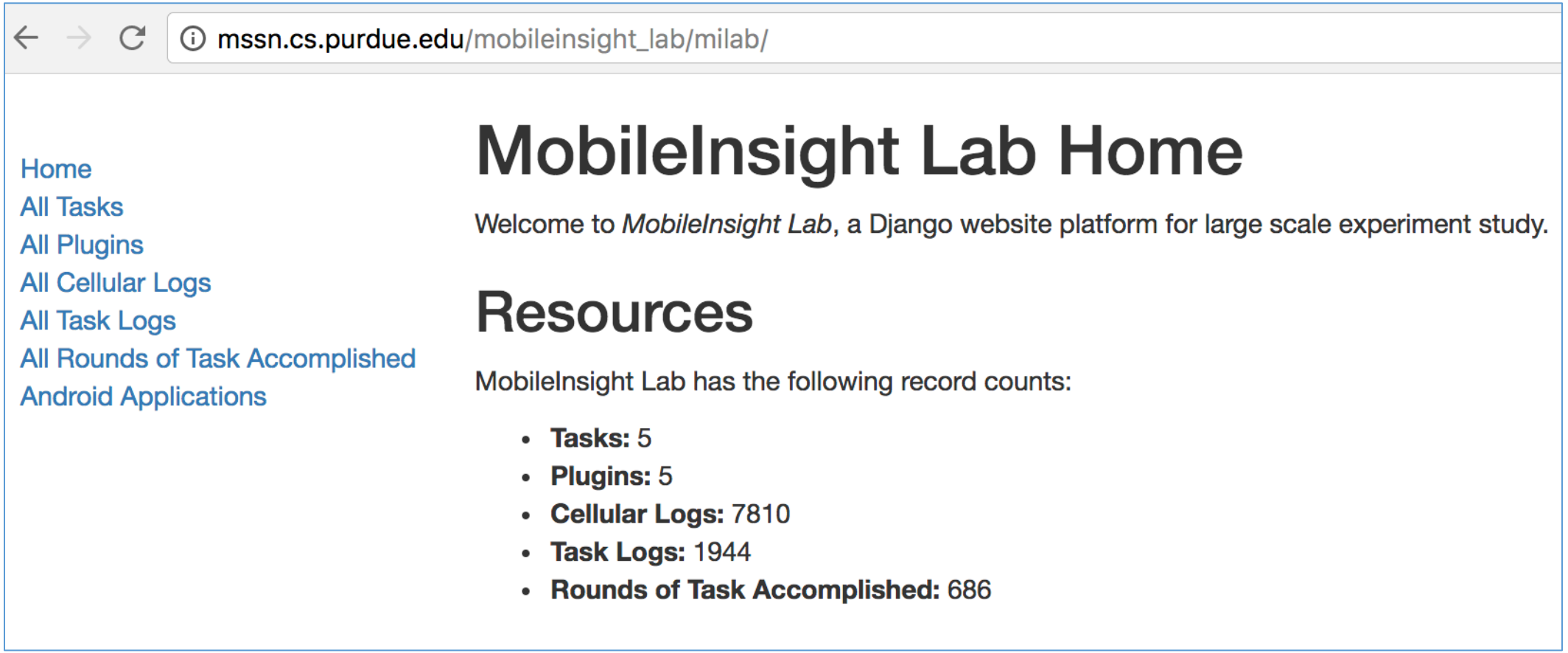
http://mssn.cs.purdue.edu/mobileinsight_lab/milab/

MiLAB: Open Experimentation Testbed



MiLAB: Open Experimentation Testbed

http://mssn.cs.purdue.edu/mobileinsight_lab/milab/



- ❑ Open testbed
- ❑ Run your experiments at scale
- ❑ Data sharing
- ❑ Community-based analytics

Embracing 5G

- 5G network is almost here
- 5G research testbeds: 5GinFire, PAWR, 5GUK, OpenAirInterface, …

- Stringent KPIs: 1Gbps, 1ms delay, 1000x, 99.999%, …

Embracing 5G

- 5G network is almost here
- 5G research testbeds: 5GinFire, PAWR, 5GUK, OpenAirInterface, …
- Stringent KPIs: 1Gbps, 1ms delay, 99.999%,
- Shed light on 5G design
  - NFV, function chaining, network slicing
- Trace-driven emulation/simulation
  - Use real-world traces to dev
    (e.g, NS-3)
  - Feed them into 5G testbeds

Open Opportunities

- **Mobile network analytics**
  - Big data
  - App KPIs: bandwidth, latency, jitter, suspension, failure, availability, …
- **Mobile network automation**
  - Analytics → action
  - E.g., failure diagnosis → recovery
  - E.g., cross-layer app optimization

Tutorial Summary

- **From simulation to practice**
  - Work on real problems over real cellular networks
- **From closeness to openness**
  - Provide open-access to fine-grained cellular network operation info at runtime
- **From data to analytics and action**
  - Monitor, analyze and exploit fine-grained cellular data
- **From individual to community**
  - Open-source, extensible tool for the community and by the community

Three Takeaways

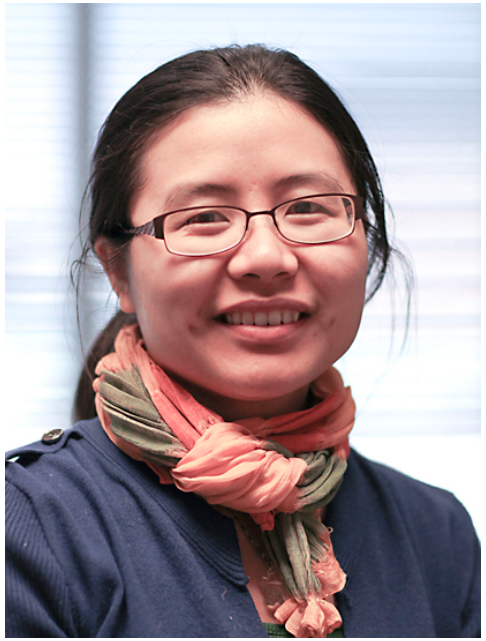
- **Towards network intelligence**
  - Cognitive network management (5G)
  - Exploit data-knowledge-action cycle with ML
- **MobileInsight: In-device network intelligence**
  - First-step: ready-to-use
  - Conduct research of your own interests
- **MiLAB: Towards a community testbed**
  - Experimentation, data, knowledge, action
  - **Join us! Make a difference**

Many Thanks to

The MobileInsight Team

Songwu Lu (UCLA)
Yuanjie Li (UCLA)
Zengwen Yuan (UCLA)
Haotian Deng (Purdue)
Jiayao Li (UCLA, Peking Univ)
Qianru Li (UCLA)
Zhehui Zhang (UCLA)
Zhehan Li (Peking Univ)
Wenguang Huang(SJTU)
Chang Zhou (SJTU)
…

MobileInsight Users and Contributors



Chunyi Peng
Assistant Prof
Purdue Univ.
chunyi@purdue.edu

NSF

http://mobileinsight.net
https://github.com/mobile-insight
http://mssn.cs.purdue.edu/mobileinsight_lab/milab
Technical support: support@mobileinsight.net

Reference: Others' Publications

[mobicom17-1] Özgü Alay, Andra Lutu, et.al, Experience: An Open Platform for Experimentation with Commercial Mobile Broadband Networks, MobiCom'17, Snowbird, Utah, Oct 2017.
[mobicom17-2] Ahmed Elmokashfi, Dong Zhou, Džiugas Baltrunas, Adding the Next Nine: An Investigation of Mobile Broadband Networks Availability, MobiCom'17, Snowbird, Utah, Oct 2017.
[mobicom17-3] Anand Padmanabha Iyer, Li Erran Li, Ion Stoica, Experience: Automating Diagnosis of Cellular Radio Access Network Problems, MobiCom'17, Snowbird, Utah, Oct 2017.
[mobisys17] Xiufeng Xie, Xinyu Zhang, Shilin Zhu, Accelerating Mobile Web Loading Using Cellular Link Information, MobiSys'17, 2017.
[globecom17] Robert Falkenberg, Karsten Heimann, Christian Wietfeld, Discover Your Competition in LTE: Client-Based Passive Data Rate Prediction by Machine Learning, Globecom'17, Singapore, 2017.
[automotive17] Ruilin Liu, Daehan Kwak, Srinivas Devarakonda, Kostas Bekris, Liviu Iftode, Investigating Remote Driving over the LTE Network, Automotive UI'17, 2017.

Reference: Our Publications (1/2)

[mobicom16] Yuanjie Li, Chunyi Peng, Zengwen Yuan, Jiayao Li, Haotian Deng and Tao Wang, *MobileInsight: Extracting and Analyzing Cellular Network Information on Smartphones*, MobiCom'16, New York, USA, Oct. 2016. Best Community Paper Award.

[sigmetrics16] Yuanjie Li, Haotian Deng, Jiayao Li, Chunyi Peng and Songwu Lu, *Instability in Distributed Mobility Management: Revisiting Configuration Management in 3G/4G Mobile Networks*, SIGMETRICS'16, France, June 2016.

[icccn16] Chunyi Peng and Yuanjie Li, *Demystify Undesired Handoff in Cellular Networks*, ICCCN'16, Waikoloa, Hawaii, Aug. 2016.

[ton17-submit] Haotian Deng, Chunyi Peng, From "Always Connected" to "Always Well Connected", submitted to TON, 2017.

[infocom16] Chunyi Peng, Yuanjie Li, Zhuoran Li, Jie Zhao and Jiaqi Xu, *Understanding and Diagnosing Real-World Femtocell Performance Problems*, INFOCOM'16, San Francisco, CA, April 2016.

[mobicom17] Yuanjie Li, Zengwen Yuan, Chunyi Peng, A Control-Plane Perspective on Reducing Data Access Latency in LTE Networks, MobiCom'17, Snowbird, Utah, Oct 2017.

Reference: Our Publications (2/2)

[nsdi16] Yuanjie Li, Haotian Deng, Chunyi Peng, Zengwen Yuan, Guan-Hua Tu, Jiayao Li and Songwu Lu, *iCellular: Device-Customized Cellular Network Access on Commodity Smartphones*, NSDI'16, Santa Clara, CA, March 2016.

[icccn17] Haotian Deng, Qianru Li, Yuanjie Li, Songwu Lu, Chunyi Peng, Taqi Raza,Zhao wei Tan, Zengwen Yuan, Zhehui Zhang, Towards Automated Intelligence in 5G Systems, ICCCN'17, Vancouver, Canada, August 2017.

[sigcomm14] Guanhua Tu, Yuanjie Li, Chunyi Peng, Chiyu Li, Hongyi Wang, Songwu Lu, *Control-Plane Protocol Interactions in Cellular Networks*, SIGCOMM'14, Chicago, Aug. 2014.

[ccs16] Guan-Hua Tu, Chi-Yu Li, Chunyi Peng, Yuanjie Li and Songwu Lu, New Security Threats Caused by IMS-based SMS Service in 4G LTE Networks, CCS'16, Vienna, Austria, Oct. 2016.

[ccs15] Chiyu Li, Guanhua Tu, Chunyi Peng, Zengwen Yuan, Yuanjie Li, Songwu Lu, Xinbing Wang, Insecurity of Voice Solution VoLTE in LTE Mobile Networks, CCS'15, Denver, Oct. 2015.

[mobicom13] Guanhua Tu, Chunyi Peng, Hongyi Wang, Chiyu Li, Songwu Lu, How Voice Calls Affect Data in Operational LTE Networks, Miami, 2013.